

Installing and Configuring

Optivity Telephony Manager Release 2.0x

NORTEL
NETWORKS

NORTEL NETWORKS™

Nortel Networks Corporation

8200 Dixie Road
Brampton, Ontario
L6T 5P6, Canada

For sales and product information,
please call 1-800-4 NORTEL.

www.nortelnetworks.com



P 0 9 8 6 9 8 7

Part No. P0986987
November 2002

Installing and Configuring Optivity Telephony Manager Release 2.0x

NORTEL
NETWORKS™

Copyright © 2002 Nortel Networks

All rights reserved. November 2002.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, SL-1, Meridian 1, Succession Communication Server for Enterprise 1000, and Optivity are trademarks of Nortel Networks.

Microsoft, MS-DOS, Windows, Windows NT, and Personal Web Server are registered trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

HP and OpenView are trademarks of Hewlett-Packard Corporation.

Intel and Pentium are trademarks of Intel Corporation.

Novell and NetWare are trademarks of Novell, Inc.

Java is a trademark of Sun Microsystems, Inc.

pcANYWHERE is a trademark of Symantec Corp.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. Optivity* Telephony Manager software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying Optivity Telephony Manager software or installing the hardware unit with pre-enabled Optivity Telephony Manager software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date the Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its

own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Revision history

Date Revised	Version	Reason for revision
June 2001	1.00	Initial Standard release coincided with the introduction of OTM 1.1.
January 2002	2.00	Upissued to coincide with the introduction of OTM Release 1.2.
November 2002	3.00	Upissued to coincide with the introduction of OTM Release 2.0.

Contents

Preface	21
Before you begin	21
Text conventions	22
Acronyms	22
Related publications	23
How to get help	26
 Chapter 1	
Initial installation tasks	27
Supported systems	28
Supported upgrade paths	28
OTM requirements	29
Meridian 1 X11 system software release and package requirements	29
OTM Server hardware requirements	30
OTM Server software requirements	31
Single (stand-alone) OTM requirements	34
OTM Windows Client requirements	35
Novell* NetWare* support	36
OTM Web Client requirements	36
Installation checklist	37
OTM Server software installation	41
Software installation procedure	43
OTM Client software installation	58
OTM upgrades	64
Upgrading the OTM Server to the same release of OTM	65
Upgrading your OTM PCs	65
Upgrading to a new release of OTM	66
Installing Web Help	71

Migrating from MAT to OTM	75
Migrating data from MAT to OTM on the same PC	75
Installing OTM on a Windows NT server being used as a MAT file server	76
Migrating data from MAT on one PC to OTM on another PC	77
Migrating data from MAT to OTM on a PC that is being upgraded to Windows 2000	78
Migrating data from MAT to OTM on a new Windows 2000 PC	78
MAT/OTM migration summary	79
Migrating CDR data from MAT to OTM	80
License management	85
TN license	85
RU license	86
Client license	87
Security device (dongle)	87
 Chapter 2	
Initial configuration tasks	89
Configuring a modem for OTM applications in Windows	90
High-speed smart modem configuration consideration	91
Troubleshooting modem connections	92
Logging in and changing the default password on Windows 98 stand-alone systems	96
Initial log in on Windows NT and Windows 2000 systems	97
Testing the connection	98
Setting up communications information	98
Setting up customer information	103
Setting up OTM applications	104
Setting up system data	106
Add sites and systems via the OTM Navigator window	106
Adding a site	106
Adding a Meridian 1 or Succession CSE 1000 Release 1.x system	108
Adding a Release 2.0 Succession CSE 1000 system	127
Adding a Generic system or device	148
Add OTM Windows users via the OTM Windows Navigator	151
Creating a user group	152
Adding a user	154

User authentication	156
Adding OTM Web Navigator users	158
User login and security	159
Access permissions	160
User authentication	162
User Groups	164
Installing and Configuring Desktop Services	174
Setting Up the Meridian 1 or Succession CSE 1000 system	180
Determining the OTM PC IP address	188
Enabling Meridian 1 and Succession CSE 1000 system alarms with LD 117 ...	188
Configuring Option 11C and Succession CSE 1000 systems for survivability	190
Configuring IP Line data for an Option 11C system	190
Configuring IP Line data for a Succession CSE 1000 system	192
Transmitting IP Line node configuration data from OTM to the IP Line cards ...	194
Setting up virtual terminal service	195
Virtual ports	195
Setting up the Data Buffering and Access application	200
Setting up the LDAP Server	201
Setting Up Alarm Management	202
Performing an OTM backup	202
OTM Web browser Client installation	204
Accessing the OTM Server Web Navigator via the PC Client	204
Integrating OTM with Optivity NMS	206
How the OTM with Optivity NMS integration works	206
Integration requirements	207
The process of OTM-ONMS integration	208
OTM OIT files	209
Checklist for installing the Optivity Integration Toolkit	209
About oit!Install	210
Using Optivity NMS InfoCenter	211
Viewing OTM Server Object Properties	216
Modifying OTM Server Object Properties	217
Starting OTM Web Applications	217
Using FaultSummary	219
Configuring OTM	221

Removing an OTM Server	222
Troubleshooting	222
Integrating OTM with HP OpenView	224
Overview	224
Limitations	225
Hardware and software requirements	226
System integration	226
Installation and configuration	229

Chapter 3

Windows NT and Windows 2000 reference 249

Installing Windows NT	249
Hardware compatibility check	250
Running the Windows NT setup program	250
Installing Windows NT components	251
Installing Network Adapter software	252
Configuring TCP/IP	253
Configuring Initial Workgroups	254
Configuring system settings	255
Creating an Emergency Repair disk	255
Completing the Windows NT installation	255
Installing Remote Access Service on Windows NT	256
Installing Windows 2000	260
Hardware compatibility check	261
Running the Windows 2000 setup program	261
Installing Windows 2000 components	262
Configuring TCP/IP	263
Installing a modem	264
Installing Remote Access Service on Windows 2000	264
Testing network cards	266
Testing the Customer LAN	266
Testing the Embedded LAN	266

Chapter 4	
Uninstall OTM	267
 Appendix A	
OTM engineering guidelines	A-1
Capacity factors	A-1
Software limits	A-3
Hard-coded limits	A-3
Operational limits	A-8
PC hardware	A-11
OTM Server hardware requirements	A-12
Single (stand-alone) OTM hardware requirements	A-13
OTM Windows Client hardware requirements	A-14
OTM Web Client hardware requirements	A-14
Physical memory	A-14
Hard disk	A-15
Processor speed	A-17
Windows NT Server and Windows NT Workstation differences	A-17
Network bandwidth	A-18
Typical configurations	A-18
Bandwidth utilization	A-22
OTM System Performance	A-24
Network impact on OTM Windows Client/Server	A-24
Hostname resolution	A-26
Telecom Billing System Display option	A-31
OTM port usage	A-34
Sample walk-through of computations	A-36
Sample configurations based on application usage and features	A-36
Sample PC and Meridian 1 configurations	A-37
Operational constraints	A-37
Configuration calculations	A-39
Index	Index-1

Figures

Figure 1	High-level outline of the installation screens	42
Figure 2	Software Installation Wizard	44
Figure 3	Software Selection dialog box	45
Figure 4	Software Selection Confirmation dialog box	45
Figure 5	Software License Agreement	46
Figure 6	Welcome	47
Figure 7	Identification	48
Figure 8	Setup Choices	49
Figure 9	Windows Installer 2.0 information box	50
Figure 10	Enter Keycodes	50
Figure 11	Destination for Application Files	51
Figure 12	Destination for Common Data Files dialog box	52
Figure 13	Destination for Local Data Files dialog box	53
Figure 14	Select Components	54
Figure 15	Summary of default applications	55
Figure 16	Applications to Install	56
Figure 17	Copy files	56
Figure 18	JRE Installation	57
Figure 19	Source for Application Executables dialog box	60
Figure 20	Source for Common Data Files dialog box	61
Figure 21	Destination for Local Data Files dialog box	62
Figure 22	Enter Keycodes dialog box	63
Figure 23	Applications to Link dialog box	64
Figure 24	Application Licenses to Upgrade	68
Figure 25	Applications to Install	69
Figure 26	Applications to Upgrade	70
Figure 27	Applications to Remove	71
Figure 28	Software Selection: Web Help	72
Figure 29	Confirmation Dialog Box	72

Figure 30	Help License	73
Figure 31	Select Web Help components dialog box	74
Figure 32	Select Web Help sub-components dialog box	74
Figure 33	MAT Migration: OTM Setup dialog box	76
Figure 34	MAT Backup Database: Choose Destination Location	77
Figure 35	Launch Call Database	81
Figure 36	Launch Archive	81
Figure 37	Archive Filter dialog box	82
Figure 38	Store the Archive file	82
Figure 39	Purge warning confirmation box	83
Figure 40	Launch Collection Configuration	83
Figure 41	TBS System Configuration—Collection tab	84
Figure 42	Start Collection dialog box	85
Figure 43	TN license warning dialog box	85
Figure 44	TN license error dialog box	86
Figure 45	Client removed dialog box	87
Figure 46	Change Password dialog box	97
Figure 47	Add Communications Profile dialog box	99
Figure 48	System Properties dialog box—Communications tab—Ethernet Profile	100
Figure 49	System Properties dialog box—Communications tab—PPP Profile . . .	101
Figure 50	System Properties dialog box—Communications tab—Serial Profile . .	102
Figure 51	System Properties dialog box—Customers tab	103
Figure 52	Customer Properties dialog box—General tab	104
Figure 53	System Properties dialog box—Applications tab	105
Figure 54	New Site Properties dialog box	107
Figure 55	Add System dialog box—Meridian 1	108
Figure 56	System Properties dialog box—General tab	110
Figure 57	Add Communications Profile dialog box	111
Figure 58	System Properties dialog box—Communications tab—Ethernet Profile	112
Figure 59	System Properties dialog box—Communications tab—PPP Profile . . .	113
Figure 60	System Properties dialog box—Communications tab—Serial Profile . .	114
Figure 61	System Properties dialog box—System Data tab	115
Figure 62	System Properties dialog box—Applications tab	117
Figure 63	System Properties dialog box—Customers tab	118
Figure 64	Customer Properties dialog box—General tab	120

Figure 65	Customer Properties dialog box—Features tab	121
Figure 66	Customer Properties dialog box—Numbering Plans tab	122
Figure 67	System Properties dialog box—Network tab	123
Figure 68	Add Survivable IP Cabinet dialog box	124
Figure 69	Survivable Cabinet System Properties dialog box—Network tab	126
Figure 70	Add System dialog box—Succession CSE 1000	127
Figure 71	System Properties dialog box—General tab	128
Figure 72	Add Communications Profile dialog box	129
Figure 73	System Properties dialog box—Communications tab— Ethernet Profile	130
Figure 74	System Properties dialog box—Communications tab—PPP Profile	131
Figure 75	System Properties dialog box—Communications tab—Serial Profile	132
Figure 76	System Properties dialog box—System Data tab	133
Figure 77	System Properties dialog box—Applications tab	135
Figure 78	System Properties dialog box—Customers tab	136
Figure 79	Customer Properties dialog box—General tab	138
Figure 80	Customer Properties dialog box—Features tab	139
Figure 81	Customer Properties dialog box—Numbering Plans tab	140
Figure 82	System Properties dialog box—Network tab	141
Figure 83	Add Associated Equipment dialog box	142
Figure 84	Add Survivable Media Gateways dialog box	143
Figure 85	Branch Office System Properties dialog box—Network tab	145
Figure 86	Gatekeeper Zones dialog box	147
Figure 87	Add System dialog box—Generic	149
Figure 88	System Properties dialog box—Applications tab for non-Meridian 1 devices	150
Figure 89	User Groups window	152
Figure 90	New User Group Properties dialog box	153
Figure 91	User Properties dialog box	155
Figure 92	User Authentication dialog box	157
Figure 93	User Authentication page	163
Figure 94	User Groups page	166
Figure 95	User Group Properties dialog box—Navigator tab	167
Figure 96	Telephone access properties dialog box—General Tab	169
Figure 97	Telephone access properties dialog box—Keys tab	171
Figure 98	Telephone access properties dialog box—Features tab	173

Figure 99	Telephone access properties dialog box—Details tab	174
Figure 100	Entering Login Name attribute	176
Figure 101	Entering User Group attribute	177
Figure 102	Entering Web Reporting Access Rights attribute	179
Figure 103	ITG IP Phones - ITG Node Properties dialog box - Ports tab	192
Figure 104	Configuring Virtual Ports (serial, logging disabled)	196
Figure 105	Configuring Virtual Ports (Meridian 1 system, logging enabled)	197
Figure 106	Configuring Virtual Ports (Telnet system, logging enabled)	198
Figure 107	Terminal Properties dialog box	200
Figure 108	OTM Backup Information dialog box	203
Figure 109	JRE Plug-in download prompt	205
Figure 110	InfoCenter Resources	213
Figure 111	InfoCenter Voice Management Properties dialog box	214
Figure 112	InfoCenter Object Properties dialog box	216
Figure 113	Starting OTM Web Applications	218
Figure 114	Modify Application Launch dialog box	220
Figure 115	Launch FaultSummary	221
Figure 116	OTM alarm integration with HP OpenView Network Node Manager	225
Figure 117	HP OpenView Network Node Manager Network Map	227
Figure 118	HP OV NNM Alarms Browser	228
Figure 119	Alarm message content	228
Figure 120	OTM Web Access	229
Figure 121	NNM Load/Unload MIBs	230
Figure 122	Load/Unload MIBs	230
Figure 123	Load MIB	231
Figure 124	NNM Main Menu - Event Configuration	232
Figure 125	Event Configuration	232
Figure 126	Modify Events - Description	233
Figure 127	Modify Events - Event Message	234
Figure 128	Modify Events - Actions	235
Figure 129	All Alarms Browser	237
Figure 130	NNM Edit - Add Object	238
Figure 131	Add Object Palette dialog box	238
Figure 132	Add Object Palette dialog box II	239
Figure 133	Add Object dialog box	240

Figure 134	Add Object - IP Map	241
Figure 135	Add Object - Set Attributes dialog box	242
Figure 136	Add Object - Selection Name	243
Figure 137	nslookup command	244
Figure 138	NNM Main Menu - Symbol Properties	244
Figure 139	Symbol Properties dialog box	245
Figure 140	Object Properties dialog box	246
Figure 141	Attributes for Object dialog box	246
Figure 142	Microsoft TCP/IP Properties dialog box	254
Figure 143	RAS Server TCP/IP Configuration dialog box	258
Figure 144	Network Configuration dialog box	260
Figure 145	Internet Protocol (TCP/IP) Properties dialog box	263
Figure 146	Incoming TCP/IP Properties dialog box	265
Figure 147	Uninstall Confirmation dialog box	268
Figure 148	Uninstall status box	268
Figure 149	Reboot request dialog box	269
Figure 150	Uninstall complete dialog box	269
Figure A-1	Too many users are connected error message	A-10
Figure A-2	Connecting OTM to legacy Meridian 1 systems (pre-Ethernet)	A-19
Figure A-3	Connecting OTM to ELAN connected Meridian 1 and Succession CSE 1000 Systems	A-20
Figure A-4	Connecting OTM to CWAN connected Meridian systems	A-21
Figure A-5	Station Administration Response Time versus Round Trip Time	A-25
Figure A-6	Station Administration Response Time versus Network Bandwidth	A-26
Figure A-7	Example of LMHOSTS file (part 1)	A-28
Figure A-8	Example of LMHOSTS file (part2)	A-29
Figure A-9	Sample HOSTS file	A-31
Figure A-10	Telecom Billing System	A-32
Figure A-11	Settings dialog box—Collection tab	A-33
Figure A-12	Settings dialog box—Costing tab	A-33
Figure A-13	Settings dialog box—Transmission tab	A-34

Tables

Table 1	Meridian 1 X11 system software release and packages	29
Table 2	OTM configurations that support Windows Clients	33
Table 3	OTM configurations that do not support Windows Clients (stand-alone) .	33
Table 4	Migration for OTM Windows NT server mode	79
Table 5	Migration for OTM in stand-alone mode	80
Table 6	Access privilege icons	154
Table 7	SDI port settings for OTM applications	181
Table 8	Legend for \$ variables in the Event Log Message	235
Table A-1	OTM capacity parameters	A-3
Table A-2	Web support on Servers and Workstations	A-9
Table A-3	PC performance by application	A-11
Table A-4	Differences between Windows NT Server and Windows NT Workstation	A-17
Table A-5	Network bandwidth usage per Meridian 1 system	A-22
Table A-6	OTM port usage	A-35
Table A-7	Maximum configuration for an Option 81 network averaging 2000 lines per system	A-38
Table A-8	Maximum configuration for an Option 11C or Succession CSE 1000 network averaging 400 lines per system	A-39

Preface

Optivity* Telephony Manager (OTM) is designed for managers of telecommunications equipment and authorized Nortel Networks* distributors. OTM provides a single point of access for management of Nortel Networks Meridian 1* and Succession Communication Server for Enterprise (CSE) 1000* systems. OTM uses IP technology to target the following key customer values:

- Single point of connectivity to Meridian 1 systems, Succession CSE 1000 systems, and related devices
- Data collection for traffic and billing records
- Collection, processing, distribution, and notification for alarms and events
- Data entry and propagation (employee names and telephone numbers shared in multiple databases)
- Windows and Web-based management applications

Before you begin

This guide is intended for Meridian 1 and Succession CSE 1000 system administrators using a Microsoft Windows*-based PC for management activities. This guide assumes that you have the following background:

- Working knowledge of the Windows NT*/Windows 2000 Server operating system
- Familiarity with Meridian 1 and Succession CSE 1000 system management activities
- Knowledge of general telecommunications concepts
- Experience with windowing systems or graphical user interfaces (GUIs)
- Knowledge of Internet Protocol (IP)

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is <code>chg suppress_alarm <n></code> where <i>n</i> is 0 = all, 1 = minor, 2 = major, 3 = critical, you enter <code>chg suppress_alarm 3</code> to suppress all alarms except critical alarms.
bold Courier text	Indicates command names and options and text that you need to enter. Example: Enter <code>prt open_alarm</code> .
<i>italic text</i>	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: For additional information, refer to <i>Using Optivity Telephony Manager</i> .
plain Courier text	Indicates command syntax and system output, for example, prompts and system messages. Example: Open Alarm destination #0 is 47.82.40.237
separator (>)	Shows menu paths. Example: Select Utilities > Backup in the Navigator window.

Acronyms

This guide uses the following acronyms:

ASP	active server page
CLAN	customer local area network
CLI	command line interface

CRS	Consolidated Reporting System
DBA	Data Buffering and Access
DN	directory number
ELAN	embedded local area network
GCAS	General Cost Allocation System
GUI	graphical user interface
IP	Internet Protocol
ITG	Internet Telephony Gateway
LAN	local area network
LDAP	lightweight directory access protocol
MAT	Meridian Administration Tools
NMS	network management system
OTM	Optivity Telephony Manager
PTY	pseudo-TTY (network port)
RAS	remote access server
RU	reporting unit
TBS	Telecom Billing System
TLAN	telephony local area network
TN	terminal number
TTY	teletype (serial port)
uid	unique identifier in LDAP synchronization
VLAN	virtual local area network

Related publications

For more information about using Optivity Telephony Manager for Meridian 1 and associated applications, refer to the following publications:

- *Using Optivity Telephony Manager* (553-3001-330)

Provides information on using the applications and features available with Optivity Telephony Manager for Meridian 1.

- *Using Optivity Telephony Manager Telemanagement Applications* (553-3001-331)

Provides information on the following optional telemanagement applications; Telecom Billing System (TBS), TBS Web Reporting, General Cost Allocation System (GCAS), Consolidated Reporting System (CRS), and Consolidated Call Cost Reports (CCCR).

- *Meridian Internet Telephony Gateway (ITG) Trunk 1.0/Basic Per-Trunk Signaling* (553-3001-116)

Describes configuration and maintenance of the 8-port ITG trunk card.

- *Meridian Internet Telephony Gateway (ITG) Trunk 2.0/ISDN Signaling Link (ISL)* (553-3001-202)

Describes configuration and maintenance of the 24-port ITG trunk card. This card appears to the Meridian 1 switch as a 24-port trunk card with ISDN Signaling Link (ISL) and D-channel signaling.

- *Meridian Internet Telephony Gateway (ITG) Line 1.0/IP Telecommuter* (553-3001-119)

Describes configuration and maintenance of the ITG line card for IP Telecommuter.

- *Meridian 1 and Succession Communication Server for Enterprise 1000 IP Line; Description, Installation, and Operation* (553-3001-204)

Describes configuration and maintenance of the ITG gateway card for the Meridian Internet Telephones, also referred to as IP telephones.

- *Meridian/Succession Companion DECT; Overview* (553-3601-103)

Provides an overview of OTM for MDECT systems.

- *Meridian/Succession Companion DECT; Installation Guide* (553-3601-203)

Provides instructions on how to install the OTM DECT application and how to configure the MDECT system on the OTM Server.

- *Meridian/Succession Companion DECT; Operation Administration and Maintenance* (553-3601-301)

Provides detailed instructions on using OTM to administer and maintain the MDECT system.

- *M3900 Series Meridian Digital Telephones; Description, Installation, and Administration* (553-3001-216)
Describes M3900 series telephones and related features. The M3904 and M3905 telephones provide access to an OTM-generated Corporate Directory.
- *Internet Terminals Guide* (553-3001-217)
Describes the i2002, i2004, and i2050 telephones and their features.
- *Software Features Guide* (553-3001-306)
Describes features associated with the Meridian 1 and Succession CSE 1000 systems. For each feature, information is provided on feature implementation, feature operation, and interaction between features.
- *Software Input/Output Guide, Administration* (553-3001-311)
Describes the prompts and responses for the Meridian 1 and Succession CSE 1000 system's command line interface (CLI). This guide includes information on overlay programs that are classified as administration overlays.
- *Software Input/Output Guide, System Messages* (553-3001-411)
Describes the meaning of the messages generated by the Meridian 1 and Succession CSE 1000 systems.
- *Software Input/Output Guide, Maintenance* (553-3001-511)
Describes the prompts and responses for the Meridian 1 and Succession CSE 1000 system's command line interface (CLI). This guide includes information on overlay programs that are classified as maintenance overlays.
- *Option 11C Planning and Installation* (553-3021-210)
Provides information on the Survivable IP Expansion (SIPE) feature for Option 11C systems.
- *Succession Communication Server for Enterprise 1000 Planning and Installation Guide* (553-3023-210)
Provides information on the Survivable IP Expansion (SIPE) feature for Succession CSE 1000 systems.

Describes the meaning of the messages generated by the Succession CSE 1000 system.

You can print selected technical manuals and release notes free of charge, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe* at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader*.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at www.nortelnetworks.com. From the main page, select Customer Support > Documentation.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Chapter 1

Initial installation tasks

This chapter contains:

- Optivity Telephony Manager (OTM) installation requirements
- A checklist that is designed for you to use as a reference when beginning a new OTM installation
- Procedures to install the OTM server software, validate the installation, and configure OTM features

OTM Server software installation begins on page 41.

A Microsoft* Windows NT* installation example to help the new Windows NT and OTM administrator get started begins on page 249. OTM is designed for use in either Windows NT, Windows 98, or Windows 2000 operating environments. Only the Windows NT and Windows 2000 environments support the server/client and web interface features of OTM.

OTM combines with Optivity Network Management System (NMS) 9.0.1 and above to give an integrated data, voice, and video network, as part of the Nortel Networks Unified Networking system. The resulting integration provides converged LAN, WAN, and voice management, and the capacity to monitor OTM server activity through Optivity NMS. See “Integrating OTM with Optivity NMS” on page 206 for more information on OTM/Optivity NMS integration procedures and requirements.

For installation recommendations that will help to create a secure environment for your OTM data and users, see “Security Management” in the Common Services chapter of *Using Optivity Telephony Manager* (553-3001-330).

To configure modems for use with OTM, refer to “Configuring a modem for OTM applications in Windows” on page 90.

For detailed hardware and software guidelines to consider when planning OTM installations, refer to Appendix A, “OTM engineering guidelines.”

Supported systems

OTM 2.0 supports the following systems:

- Succession CSE 1000 Releases 1.0 - 2.0
- Meridian 1 Options 11C, 51C, 61C, 81, and 81C running X11 Releases 19 - 25.40
- Meridian 1 Option 11C Compact systems running X27 Releases 1 - 2
- Meridian 1 Option 11C Mini systems running X11 Releases 24.24 - 25.40
- Meridian ITG Trunk 1.0 (IP Telephony/ M1 IP Trunks)
- Meridian ITG Line 1.0 (IP M1 Telecommuter)
- Meridian ITG Trunk 2.x (IP ISDN IP Trunks)
- Meridian ITG Line 2.x (IP Phones)
- MDECT (DMC8 card, and DMC4 with updated loadware)
- IP Trunk 3.0 on Meridian 1
- IP Line 3.0 on Meridian 1

Supported upgrade paths

OTM 2.0 supports direct upgrades from MAT 6.67, OTM 1.0, OTM 1.01, OTM 1.1, and OTM 1.2.

Customers on MAT releases 5.x or 6.x (not including MAT 6.67) are provided with a single order code that follows a two-step upgrade path. You first upgrade to MAT 6.67, and then to OTM 2.0.

Customers on a release of MAT prior to MAT 5.x should install OTM 2.0 as a new installation.

OTM requirements

OTM requirements include:

- “Meridian 1 X11 system software release and package requirements”, next
- “OTM Server hardware requirements” on page 30
- “OTM Server software requirements” on page 31
- “Single (stand-alone) OTM requirements” on page 34
- “OTM Windows Client requirements” on page 35
- “OTM Web Client requirements” on page 36

Meridian 1 X11 system software release and package requirements

In general, OTM requires no special X11 system software release to run. Table 1 is a list of X11 releases and required packages based on the OTM applications.

Table 1 Meridian 1 X11 system software release and packages

OTM application	Minimum X11 release required	X11 pkgs required
Alarm Management	X11 R22 or later	Pkg 164, 242, 243, and 296
-Additional pkgs for Alarm Notification		Pkg 55 and 315
Maintenance Windows	X11 R22 or later	Pkg 164, 242, 243, and 296
System Terminal - Overlay Passthru	X11 R22 or later	Pkg 164, 242, and 296
Ethernet connection (for Station Administration, Traffic Analysis, and ESN ART)	X11 R22 or later	Pkg 164, 242, and 296
SNMP Alarms (Open Alarms)	X11 R22 or later	Pkg 315
Data Buffering and Access - Ethernet	X11 R24 or later	Pkg 351
Data Buffering and Access - Serial	N/A	N/A
M1 Database Disaster Recovery	X11 R24 or later	Pkg 164, 242, 296, and 351
Virtual Terminal Server	X11 R22 or later for access over IP	Pkg 164, 242, and 296

OTM Server hardware requirements

The OTM Server must meet the following minimum hardware requirements. Refer to Appendix A, "OTM engineering guidelines," for more information on OTM Server hardware requirements.



Note: This information is subject to change. For the latest system requirements, see the OTM General Release Bulletin.



Note: Response time testing is based upon the recommended configuration, not the minimum configuration. Response time performance is only supported on the recommended configuration.

- Intel® Pentium® II Processor 400 MHz CPU minimum; Intel Pentium III Processor 600 MHz CPU recommended
- 2 GB hard drive or greater (1000 MB free space plus customer data storage requirements)
- 256 MB of RAM minimum; 512 MB of RAM recommended
- CD-ROM drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA color monitor and interface card (800 X 600 resolution for graphics)
- Two Ethernet Network Interface cards required to support connection with the Meridian 1 via Ethernet and Customer LAN
- An optional Hayes-compatible modem used for connection to remote systems, required for polling configurations (56 K BPS recommended)



Note: OTM does not support software-based WinModems.

- PC COM port with 16550 UART
- Printer port (LPT) required for dongle
- Dongle (for server or stand-alone only)

- Windows-compatible mouse or pointing device (PS/2 mouse preferred to free up a PC serial port)



Note: Do not install OTM on a Microsoft Windows NT or Windows 2000 system that is configured as a primary domain controller (PDC).

OTM Server software requirements

OTM requires a Windows NT 4.0 or Windows 2000 Server, or a Windows NT Workstation or Windows 2000 Professional with the following software:

- TCP/IP Protocol
- Remote Access Service
- Java 1.3.1 runtime environment
- NT Server 4.0, Service Pack 6a, and Option Pack 4 (for Windows NT)



Note: Windows NT Workstation and Windows 2000 Professional do not support Windows Clients.

The required components from Option Pack 4 are:

- Internet Information Server (IIS) 4.0 or above



Caution: ITG file transfers may fail if there is another file transfer protocol (FTP) service running on the OTM Server. By default, IIS will install the FTP Publishing Service. This service may be set to start automatically and will cause ITG applications to fail.

- Microsoft Transaction Server
- Microsoft Data Access Components (MDAC)
- Microsoft Management Console (NMC)

— NT Option Pack Common Files



Note: Chapter 3, “Windows NT and Windows 2000 reference,” on page 249 provides detailed information on installing and configuring Windows NT for use with OTM.

- Windows 2000 Server, and Service Pack 3 (for Windows 2000)
 - Microsoft Internet Explorer 5.0, 5.5, or 6.0, Netscape Communicator 4.7x
-



Note: Element Management for the Succession CSE 1000 system requires Microsoft Internet Explorer. Netscape Communicator 4.7x will not allow you to launch Element Management.



Note: Netscape 6.x or later as well as Netscape Navigator 4.08 and earlier are not supported by OTM.

- Network card drivers
-



Note: Ask the network card manufacturer about the type of network card and the availability of the required software driver.

Support for Microsoft Windows 2000™

OTM 1.01 introduced support for the Windows 2000 operating system. The following configurations are supported:

- Windows 2000 Server as an OTM server
- Windows 2000 Server as an OTM server with a combination of Windows 98, Windows NT 4.0 Workstation, or Windows 2000 Professional as clients
- Windows 2000 Professional as an OTM stand-alone PC
- Windows 2000 Professional as an OTM Web server

The following configuration of OTM is not supported on Windows 2000:

- Windows 2000 Professional as an OTM Windows file server

Configuration support based on operating system

The ability to support OTM Windows Clients in a Client-Server relationship is dependent upon the operating system installed on the OTM Server.

Table 2 outlines configurations that support both Windows and Web Clients.

Table 2 OTM configurations that support Windows Clients

OTM Server OS	Supported OTM Windows Client OS	Supported Web Client browsers
Windows NT 4.0 Server	Windows 98 Windows NT 4.0 Workstation Windows 2000 Professional	Internet Explorer 5.0, 5.5, 6.0 Netscape Communicator 4.7x
Windows 2000 Server	Windows 98 Windows NT 4.0 Workstation Windows 2000 Professional	Internet Explorer 5.0, 5.5, 6.0 Netscape Communicator 4.7x

Table 3 outlines configurations that support Web Clients but do not support Windows Clients. These OTM configurations are also referred to as stand-alone configurations.

Table 3 OTM configurations that do not support Windows Clients (stand-alone)

OTM Server OS	Supported OTM Windows Client OS	Supported Web Client browsers
Windows 98	Not supported	Not supported
Windows NT 4.0 Workstation	Not supported	Internet Explorer 5.0, 5.5, 6.0 Netscape Communicator 4.7x (see note)
Windows 2000 Professional	Not supported	Internet Explorer 5.0, 5.5, 6.0 Netscape Communicator 4.7x (see note)



Note: The number of Web Clients that can simultaneously access the OTM Server is dependent upon settings in Internet Explorer or Netscape Navigator. Windows NT 4.0 Workstation and Windows 2000 Professional allow a maximum of ten connections; however, a single Netscape Web Client session may use as many as six of these connections. This can reduce the number of simultaneous Web Clients to one. For this reason, Nortel Networks recommends that you not run more than one Web Client when OTM is installed under the Windows NT 4.0 Workstation or Windows 2000 Professional OS.



Note: The Windows 98 OS does not support the OTM DECT application.

Single (stand-alone) OTM requirements

An OTM system operating in stand-alone mode (a single web-based Client and no Windows Clients) requires the following:

- 233 MHz Intel Pentium II Processor or equivalent minimum (Pentium II running at 300 MHz is minimum for Telecom Billing System application); 400 MHz or higher Intel Pentium III recommended
- 2 GB hard drive with 500 MB of free space
- 256 MB of RAM minimum; 512 MB of RAM recommended
- Ethernet Network Interface Card
- Windows 98, Windows 2000 Server, Windows 2000 Professional, or Windows NT Workstation 4.0 or Server
- OTM dongle
- Printer port (LPT) required for dongle
- OTM CD and keycode
- Remote Access Service (RAS) (optional)
- Modem(s) for remote access (optional)

OTM Windows Client requirements

An OTM Windows Client (a computer that accesses the OTM Windows-based application on the OTM Server) requires the following:

- Intel Pentium II 233 MHz or higher CPU (Pentium II 300 MHz for running Telecom Billing System) minimum; Intel Pentium III 400 MHz or higher CPU is recommended
- 2 GB hard drive with 500 MB of free space
- 128 MB of RAM minimum; 256 MB of RAM is recommended
- CD-ROM drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA color monitor and interface card (800 X 600 resolution for graphics)
- Ethernet Network Interface
- Windows-compatible mouse or pointing device
- Windows 98, Windows 2000 Professional or Server, or Windows NT 4.0 Workstation or Server



Note: On December 31, 2001, Microsoft placed the Windows 95 operating system into a non-supported phase. The OTM Windows Client is not supported on the Windows 95 operating system beginning with OTM 2.0.

- The correct Java Runtime Environment (currently version 1.3.1) installed on the client machine
- A Microsoft Active Server Page (ASP) and HTML-compliant Web browser
- Service Pack 6a for Windows NT systems, or Service Pack 3 for Windows 2000 systems
- TCP/IP Protocol
- Remote Access Service
- Network card drivers
- Dial-up Networking for Windows 98

Windows Client performance

A number of variables impact the speed at which activities are performed on an OTM Windows Client. Some of these variables include:

- The amount of RAM on the OTM Client PC
- The OS platform in use on the OTM Client PC
- The number of TNs being managed through the Station Administration application
- Other applications that may be running on the OTM Client PC, including those that run in the background such as antivirus software
- The amount of traffic on the LAN
- The NIC on the OTM Client PC
- Deployment in the network architecture (topology and placement of the OTM Client PC with respect to the OTM Server)

Novell* NetWare* support

OTM 1.1 introduced support for Novell NetWare Release 5.x on the OTM platform. The following two Novell NetWare Client versions are supported as OTM Clients in an OTM installation:

- Novell NetWare Client 3.3 — supports Windows 98
- Novell NetWare Client 4.8 — supports Windows NT and Windows 2000



Note: The OTM Server is not supported on a Novell server. TCP/IP communication is supported. IPX/SPX communication is not supported.

OTM Web Client requirements

You can launch the OTM Web Client from a browser on any OS that supports the Java 1.3.1 Runtime Environment.

The Java 1.3.1 Runtime Environment plug-in is available as part of the OTM installation process. Internet Explorer 5.0, 5.5, or 6.0, or Netscape Communicator 4.7x is also required.



Note: Netscape 6.x or later as well as Netscape Navigator 4.08 and earlier are not supported.

To guarantee simultaneous access by more than one Web Client, you must load the OTM software onto a system running the Windows NT 4.0 Server or Windows 2000 Server OS. See the note on page 34 for more information.

Installation checklist

Use the following quick reference as a checklist or reminder when starting a new OTM installation.

Meridian 1 installation requirements

Software and memory:

- ☐ Required X11 packages (296, 315, and 351 depending on applications being installed)
- ☐ Minimum of 48 MB of memory on the Meridian 1

For Ethernet connections:

- ☐ X11 Release 22 or later
- ☐ Release 24B or later for Data Buffering and Access
- ☐ IOP, IOP/CMDU, or IODU/C cards for Options 51C, 61C, 81, 81C
- ☐ Ethernet AUI cables to be attached to each IOP (Options 51C, 61C, 81, 81C)
- ☐ NTDK27 Ethernet cable for Option 11C
- ☐ Transceivers to connect to the LAN
- ☐ Router

For PPP connections:

- ☐ Hayes compatible modem
- ☐ SDI port available on the Meridian 1 (configured for SCH only)
- ☐ Serial cable to connect the modem to the SDI port

For serial connections:

- [] SDI port available on the Meridian 1 (configured for SCH only)
- [] Hayes compatible modem for remote connection (optional)
- [] Serial cable to connect the modem to the SDI port

Programming the Meridian 1:

- [] Enable Name Option in LD 17.
- [] Define Limited Access Password in LD 17.
- [] For Serial communication: Configure a TTY with User = SCH in LD 17.
- [] For Ethernet or PPP communication: Configure a pseudo TTY (PTY) with User = SCH in LD 17.
- [] Configure Ethernet at the Meridian 1 in LD 117.
- [] Define the Gateway (router) IP address on the Meridian 1 in LD 117.
- [] Configure PPP at the Meridian 1 in LD 117.
- [] INIT the Meridian 1.
- [] Enable the new IP address (defined in LD 117) in LD 137.
- [] Enable Database Disaster Recovery (DDR) in LD 117.
- [] Set open alarm destination in LD 117.
- [] Set up Data Buffering and Access in LD 177.
- [] Set up filtering in the Meridian 1 to filter out information and minor messages.

PC/Server installation requirements

Single (stand-alone) OTM installation:



Note: Stand-alone mode consists of a single web-based Client and no Windows Clients.

- [] 233 MHz Intel Pentium II Processor or equivalent minimum (Pentium II running at 300 MHz is minimum for Telecom Billing System application); 400 MHz or higher Intel Pentium III recommended
- [] 2 GB hard drive with 500 MB of free space
- [] 256 MB of RAM minimum; 512 MB of RAM recommended
- [] Ethernet Network Interface Card
- [] Windows 98, Windows 2000 Server, Windows 2000 Professional, or Windows NT Workstation 4.0 or Server
- [] OTM dongle
- [] Printer port (LPT) required for dongle
- [] OTM CD and keycode
- [] Remote Access Service (RAS) (optional)
- [] Modem(s) for remote access (optional)



Note: If multiple web Clients are connected to the stand-alone system, the requirements are equivalent to the OTM Server requirements.

OTM Server installation:

- [] 400 MHz Intel Pentium II Processor or equivalent minimum; 600 MHz or higher Intel Pentium III recommended
- [] 3 GB hard drive (1 GB of free space plus customer data storage requirements)
- [] 256 MB of RAM minimum; 512 MB of RAM recommended
- [] Two Ethernet Network Interface Cards
- [] PC COM port with 16550 UART

- [] Hayes compatible modem (optional)
- [] Windows NT Server 4.0 and Service Pack 6a; or Windows 2000 Server and Service Pack 3
- [] Windows NT Option Pack 4 or Windows 2000 Server
- [] Remote Access Service
- [] OTM Dongle
- [] OTM CD and Keycode
- [] Configure and test network interfaces
- [] Enable IP routing (if applicable)

OTM Client installation:

- [] **Windows Client** - 233 MHz Intel Pentium II Processor or equivalent (300 MHz Pentium II required for Telecom Billing System application) minimum; 400 MHz or higher Pentium III processor recommended
Web Client - 160 MHz Intel Pentium Processor or equivalent
- [] 2 GB hard drive with 500 MB of free space
- [] **Windows Client** - 128 MB of RAM minimum (256 MB of RAM recommended for improved performance and for the Billing Enhanced level applications)
Web Client - 32 MB of RAM
- [] **Windows Client** - PC COM port with 16550 UART
- [] Ethernet Network Interface Card
- [] Windows 98, Windows 2000, or Windows NT Workstation 4.0 or Server
- [] **Windows Client** - Remote Access Service
- [] **Windows Client** - OTM CD and Keycode (no Dongle required)
- [] **Web Client** - Java Runtime Environment (JRE) 1.3.1, and Microsoft Internet Explorer 5.0, 5.5, or 6.0 or Netscape Navigator 4.7

OTM Server software installation

This section describes the OTM Server software installation. The OTM software installation program uses a standard Windows “Wizard” method of user interaction. Before installing OTM, you must log on to Windows NT as an Administrator.



Note: Operating systems are typical targets of security attacks. OTM runs on a Microsoft operating system platform. Nortel Networks recommends that you visit the Microsoft Web site at <http://www.microsoft.com/technet/> for critical security updates prior to installing OTM.



Note: The OTM installation wizard does not install the index server (IIS), but other applications may have done so. Ensure that you install the Code Red Worm IIS patches as advised through Product Bulletin 2001-060 available on the Partner Information Center Web site.



Note: Before installing OTM software, exit all Windows programs and disable any virus detection software.



Note: For network installations, you must close all OTM Client sessions. This includes both Windows and Web clients.



Note: OTM requires that a drive labeled “C” exist on the server. Although the OTM software can be installed on any drive, there are some dependencies on the C drive. In particular, the directory C:\dbcnv is always created during installation and removed at the end of the installation process.



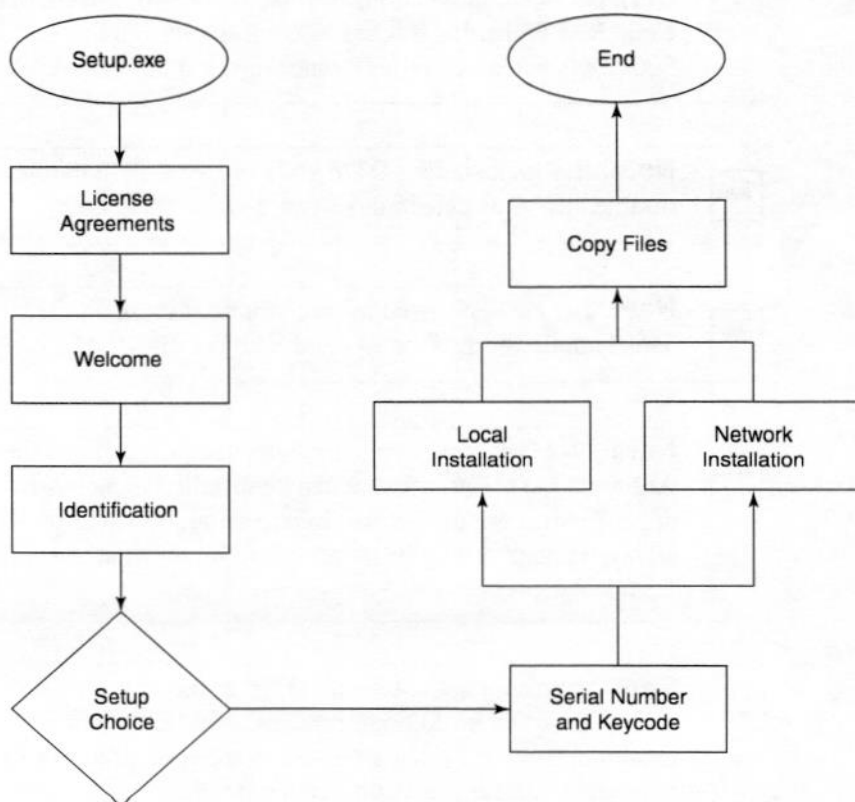
Caution: You must not install OTM in the root directory (for example, C:\). During the installation process, you must specify a folder (for example, C:\Nortel). If you install in the root directory, OTM uninstall attempts to delete everything on the drive.

➔ **Note:** Windows Installer 2.0 is required for OTM to run correctly. If the OTM installation program detects that it is not installed, the installation program will install it and then proceed with the OTM installation.

➔ **Note:** During the installation process, OTM adds the Default, EndUser and HelpDesk user groups to the server. User groups cannot have the same name as a local user on the OTM Server. If the installation program detects a local user with the same name as one of the user groups that it is attempting to add, you are given the option of renaming or deleting the local user or canceling the creation of the user group.

Figure 1 presents a high-level outline of the installation screens.

Figure 1 High-level outline of the installation screens



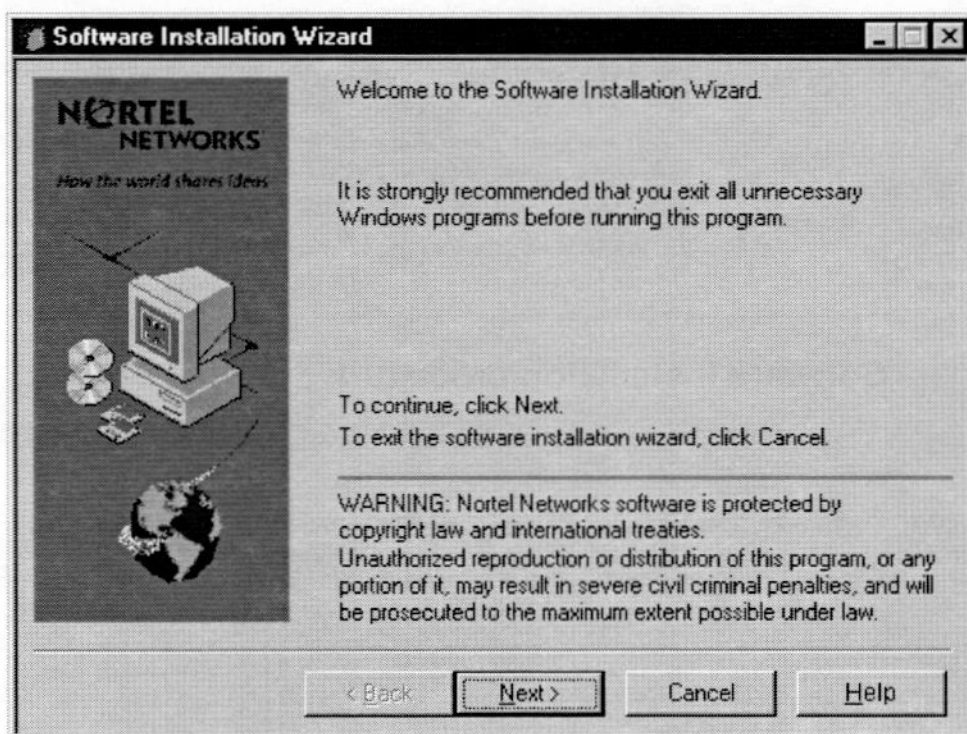
9960EA



Note: At the beginning of OTM software installation, the setup program checks for various prerequisites, and displays appropriate messages if one or more required components are not present. Additionally, a log records all errors. During installation, the log resides in the following directory path: *C:\NortelLog\log.txt*. After installation, the log resides in the local directory path where you installed the application. For each error or event, the log lists an “Event type” (Info, Warning, Critical, or Major), and “Message” (for example, “Service Pack 6a is not installed”).

Software installation procedure

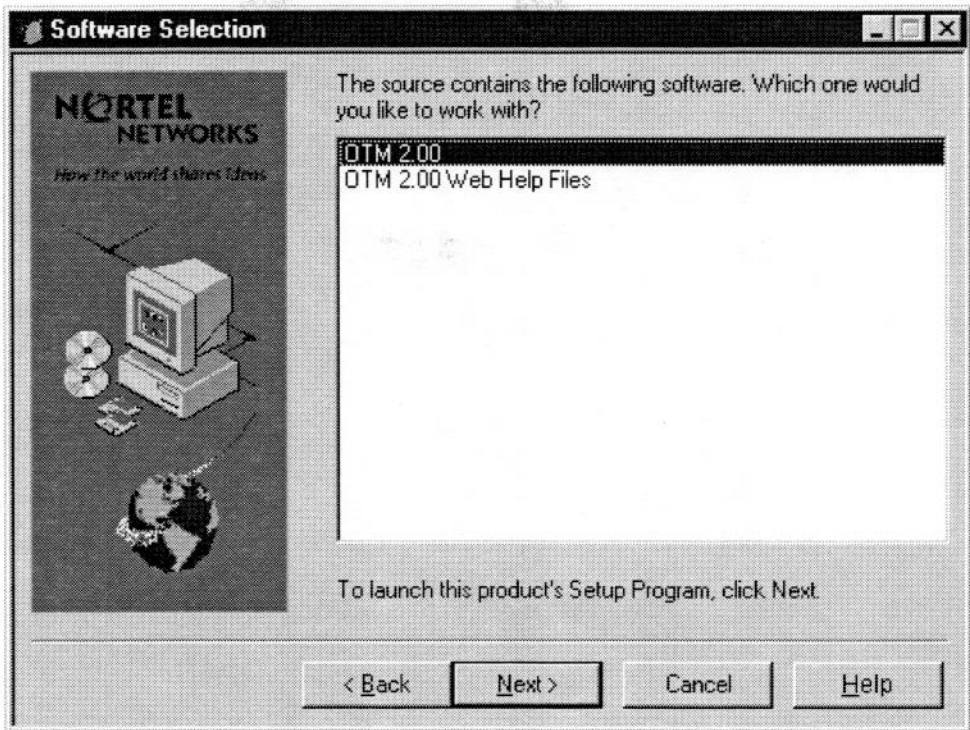
- 1 Before installation, make sure that you remove the *MAT.exe* shortcut file in the *Start up* folder, if present.
- 2 Double-click the *Setup.exe* file on the OTM CD-ROM.
The welcome screen appears (Figure 2).

Figure 2 Software Installation Wizard

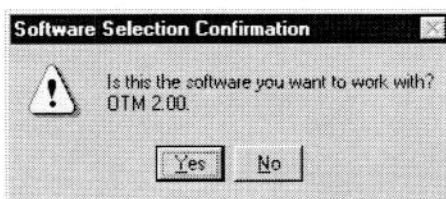
- 3** Click Next to continue.

The Software Selection dialog box appears (Figure 3).

- 4** Click to select OTM 2.00. The other option is OTM Web Help files. You can install OTM Web Help once the OTM Application installation is complete.
- 5** Click Next to continue.

Figure 3 Software Selection dialog box

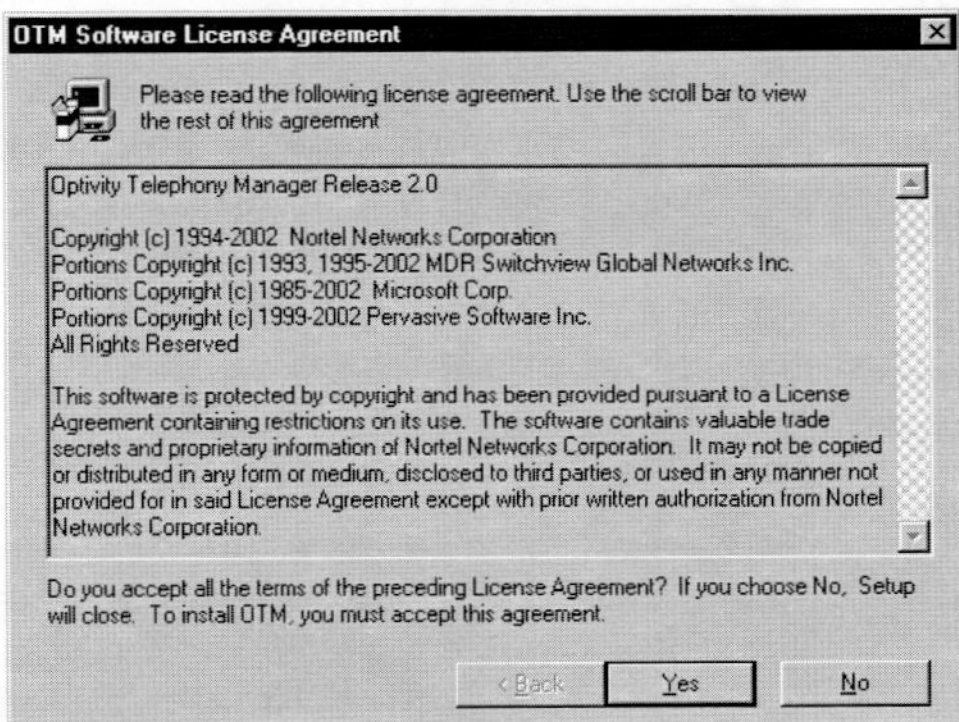
The Software Selection Confirmation dialog box (Figure 4) opens to request confirmation that OTM 2.00 is the software that you want to work with.

Figure 4 Software Selection Confirmation dialog box

- 6 Click Yes to continue.

Software License Agreement

- 7 The "Software License Agreement" opens (Figure 5). Read the Software License Agreement. Click Yes to accept the agreement.

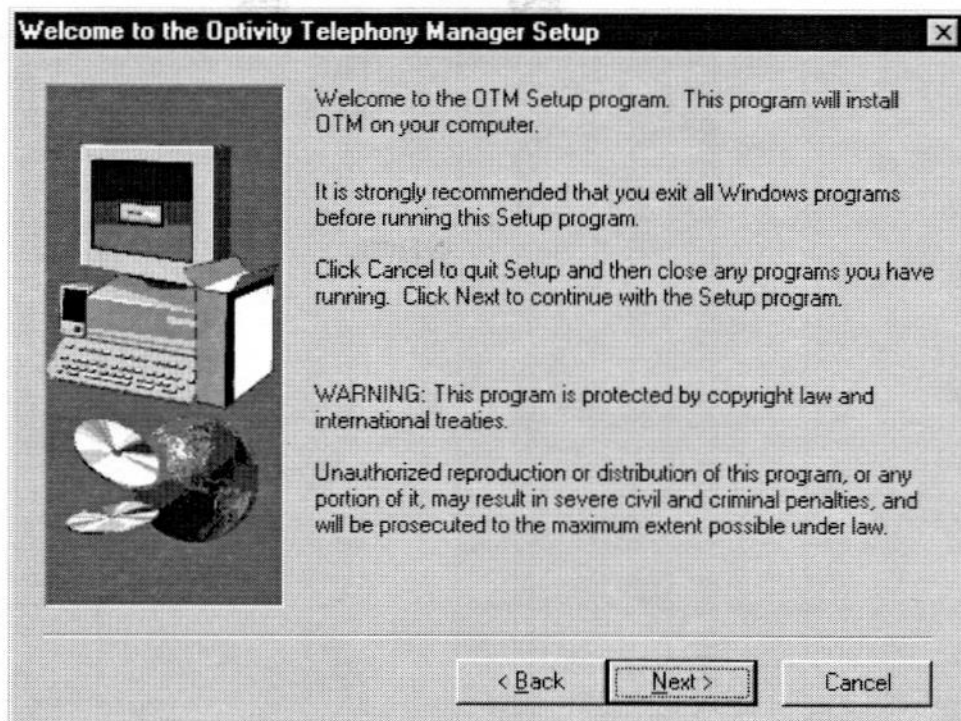
Figure 5 Software License Agreement

Welcome

The "Welcome" screen (Figure 6) welcomes you to the OTM installation program.

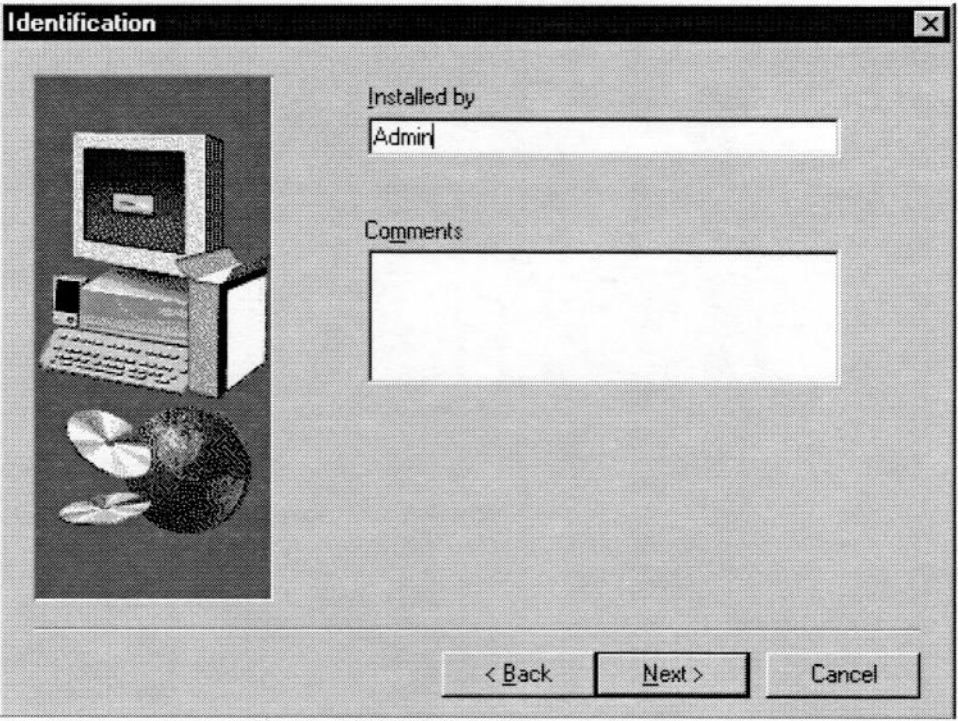
- 8 Click Next to continue.

Figure 6 Welcome



Identification

- 9 Specify the name of the person performing the installation and, optionally, a comment about the installation (Figure 7). Click Next to continue.

Figure 7 Identification

Identification

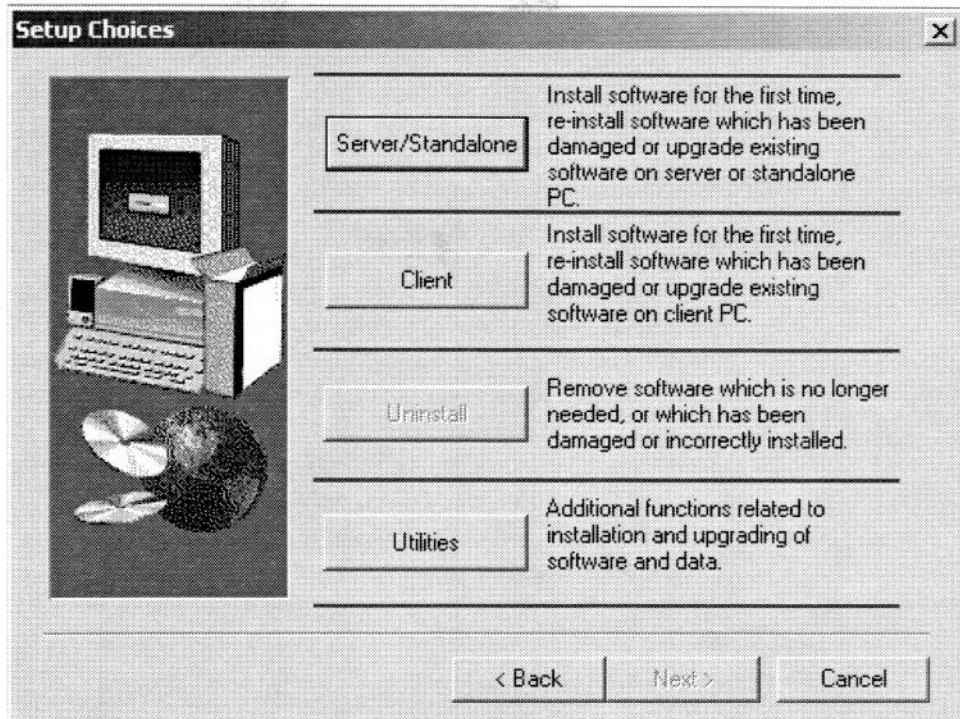
Installed by
Admin

Comments

< Back Next > Cancel

Setup Choices

- 10** For installation on an OTM Server, select Server/Standalone (Figure 8). For installation on a Client PC, select Client and see “OTM Client software installation” on page 58.

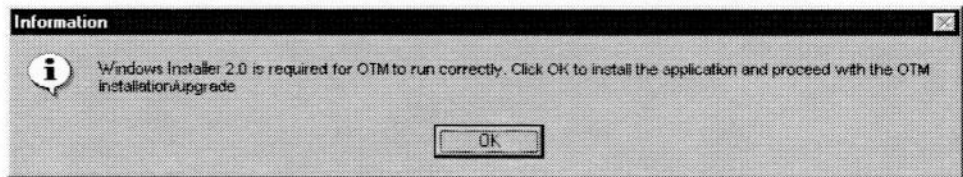
Figure 8 Setup Choices

Note: Selecting Server/Standalone will not resolve problems with damaged software. To resolve a damaged software problem, back up your data files and perform an Uninstall. Next, perform an installation, and then restore your data. See Table 5 on page 80.

Select Client to install an OTM client. The client has applications/executables, but uses the common data from the OTM Server. You must have the OTM Server software installed prior to installing the client software.

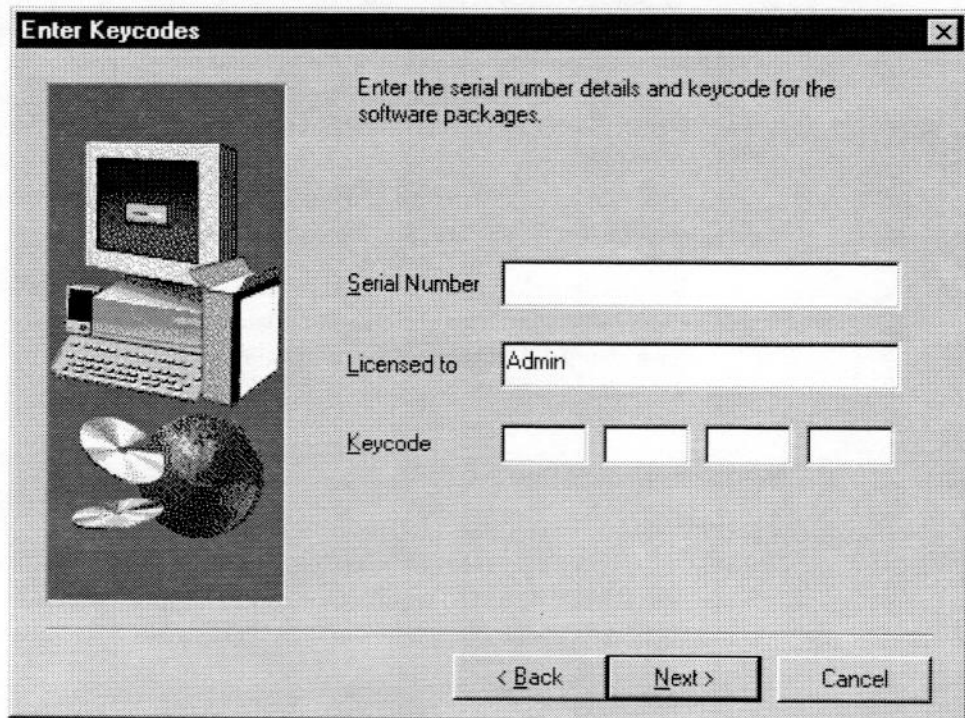
Windows Installer 2.0

- 11 OTM requires Windows Installer 2.0. If the installation wizard detects that Windows Installer 2.0 is not installed, the information box shown in Figure 9 appears. Click OK. OTM installation continues after Windows Installer 2.0 installation has been completed, and the system has been rebooted.

Figure 9 Windows Installer 2.0 information box

Serial Number and Keycode

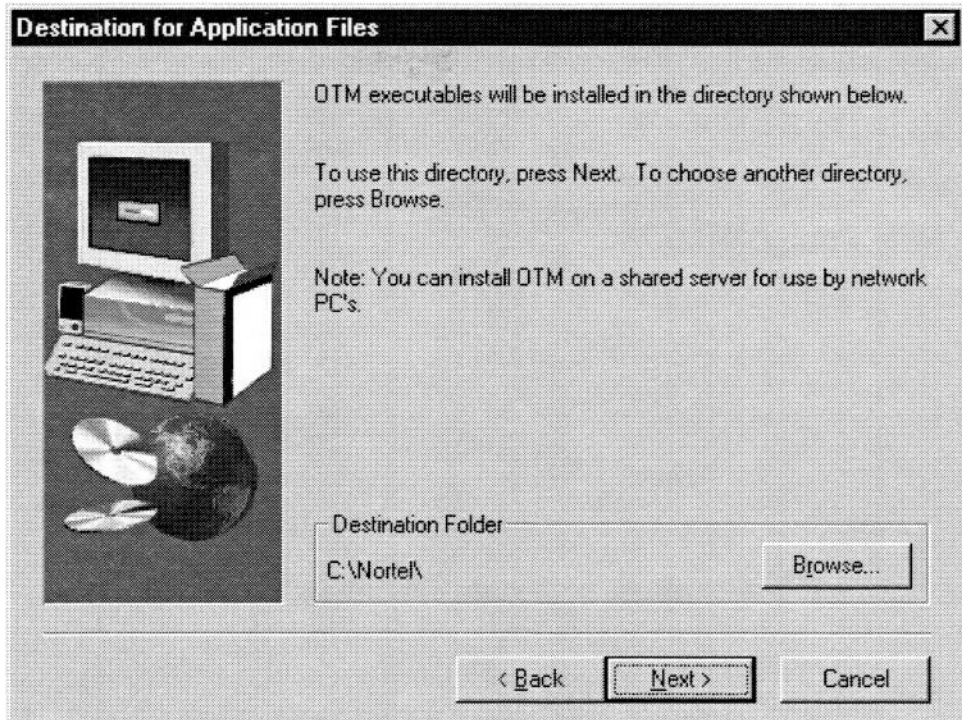
- 12** Enter the serial number and keycode that you received with your OTM software package in the Enter Keycodes dialog box (Figure 10). The serial number and keycode determine which applications are installed during the software installation process. The serial number and keycode also determine the maximum number of terminal numbers (TNs), or sets (telephones), and OTM Clients that can be configured in your OTM system. In determining your maximum number of TNs, only telephone TNs and virtual TNs are counted. Trunk TNs are not included. To purchase licensing for additional TNs or Clients, contact your OTM vendor. Click Next to continue.

Figure 10 Enter Keycodes

Destination for Application files

- 13** Specify the root directory for installing OTM Application files. Use the default directory or browse to specify a different location, as shown in Figure 11. Click Next to continue.

Figure 11 Destination for Application Files

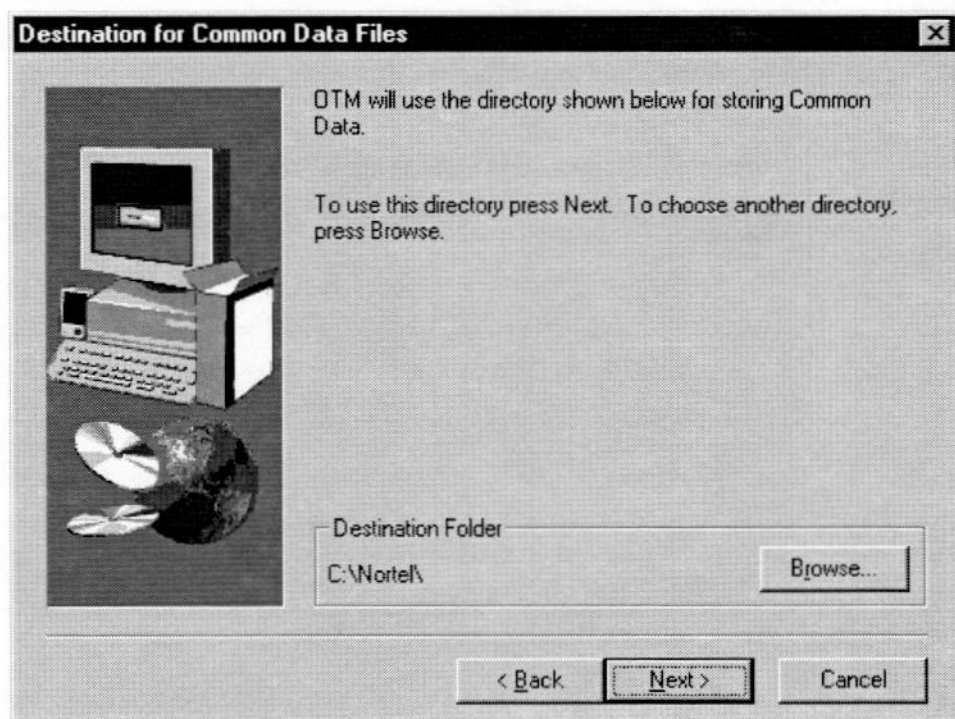


Destination for Common Data files

- 14** Specify the root directory for installing OTM Common Data files (Figure 12). Use the default directory or browse to specify a different location. The directory defaults to the path defined in step 13. Click Next to continue.

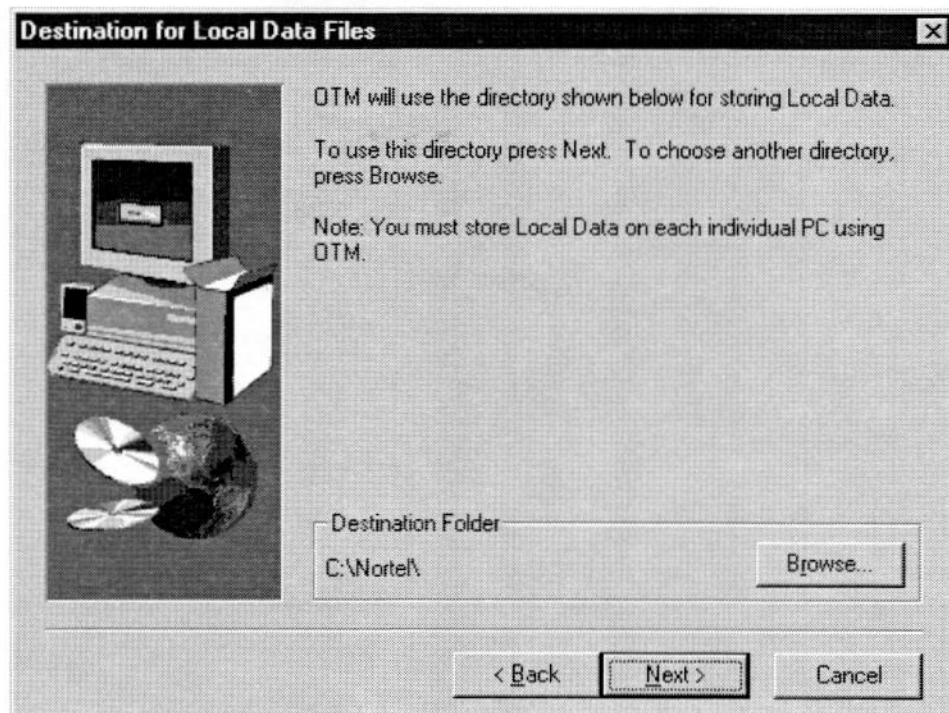


Caution: You must specify a local drive for Common Data files storage to avoid the access problems that can arise with networked drives. The installation process checks your system and prevents you from specifying a networked drive.

Figure 12 Destination for Common Data Files dialog box

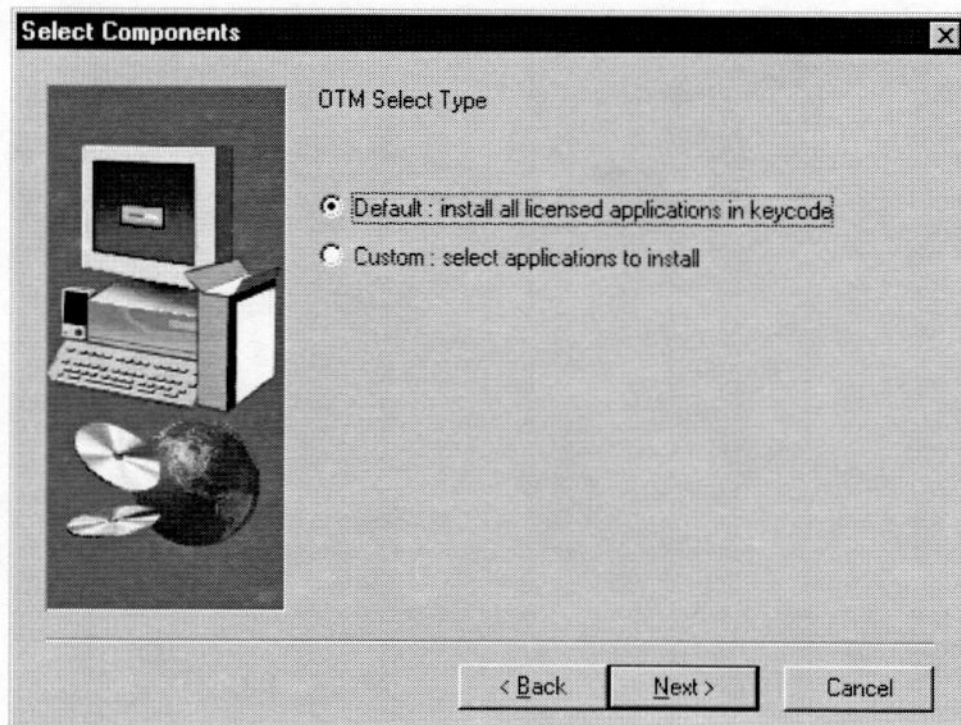
Destination for Local Data files

- 15** Specify the root directory for installing OTM Local Data files (Figure 13). Use the default directory or browse to specify a different location. The directory defaults to the path defined in step 13. Click Next to continue.

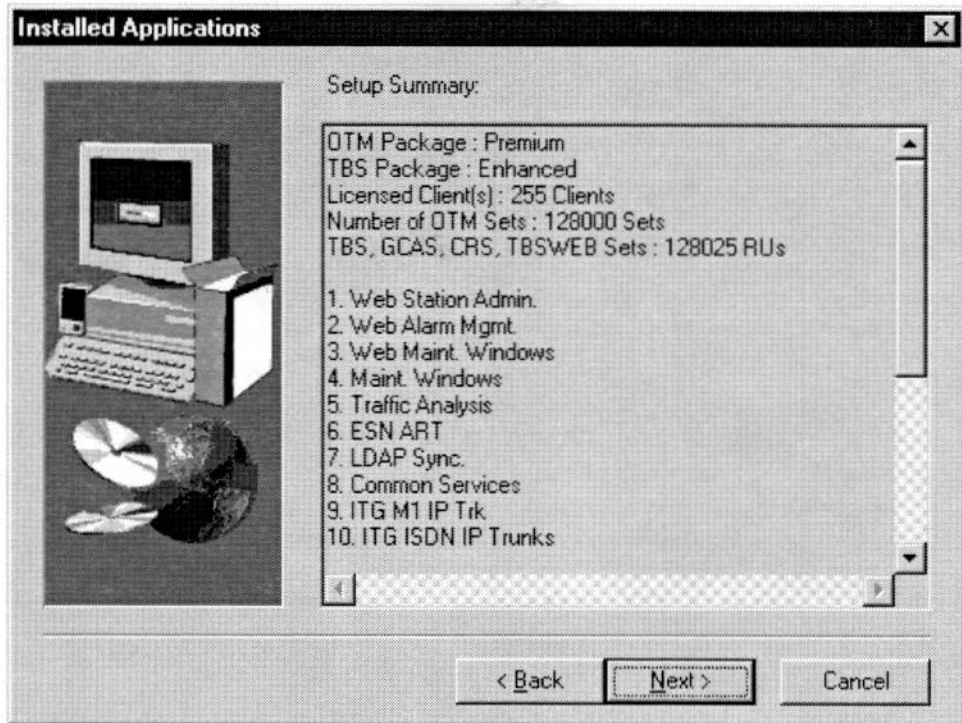
Figure 13 Destination for Local Data Files dialog box

Installation options

- 16** Specify Custom or Default installation. Select Default to install all purchased applications; select Custom to select the OTM applications that you want Setup to install (Figure 14).

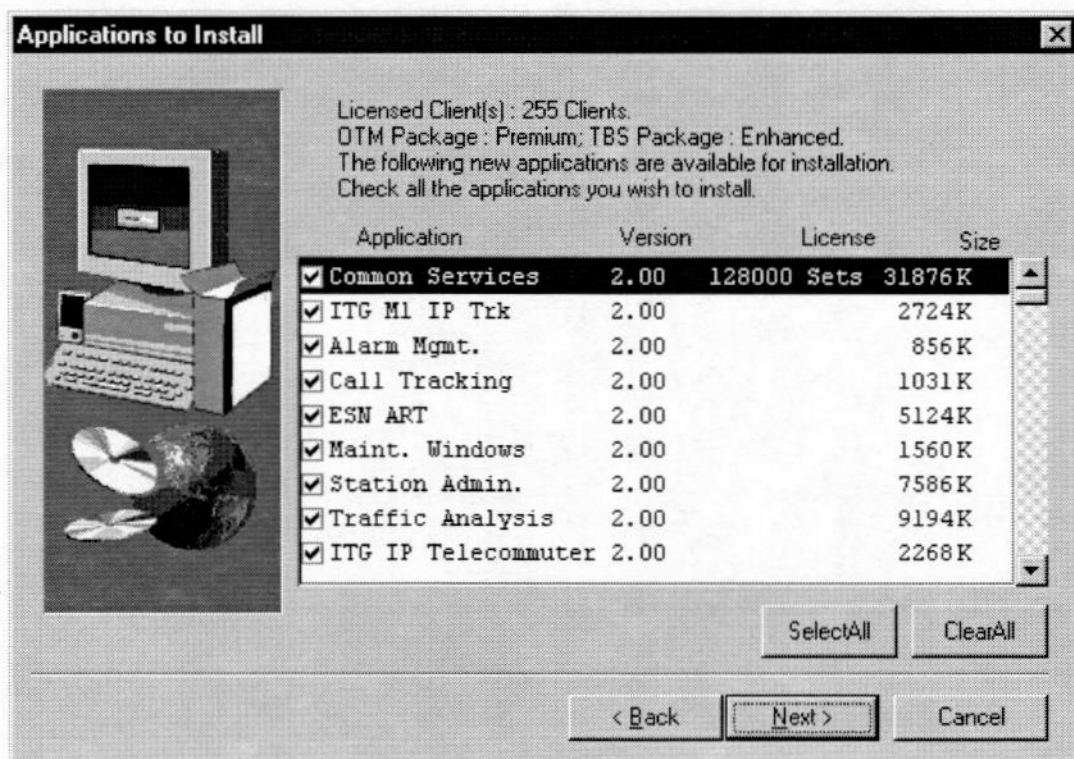
Figure 14 Select Components

If you select Default, a summary of the default applications for the level of OTM that you have purchased appears (Figure 15).

Figure 15 Summary of default applications

Applications to Install

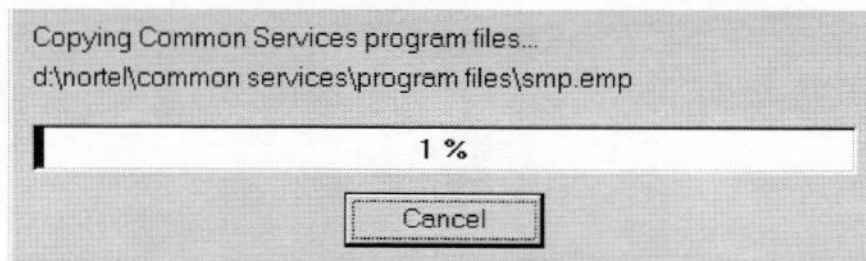
- 17** If you selected Custom, you are given a list of applications to install (Figure 16). Check the appropriate applications.

Figure 16 Applications to Install

18 Click Next to continue.

Copy files

This dialog box displays the percentage status of OTM installation, which application files are being copied, and their locations (Figure 17).

Figure 17 Copy files

Read Me File

This dialog box prompts you to read the readme.txt file.

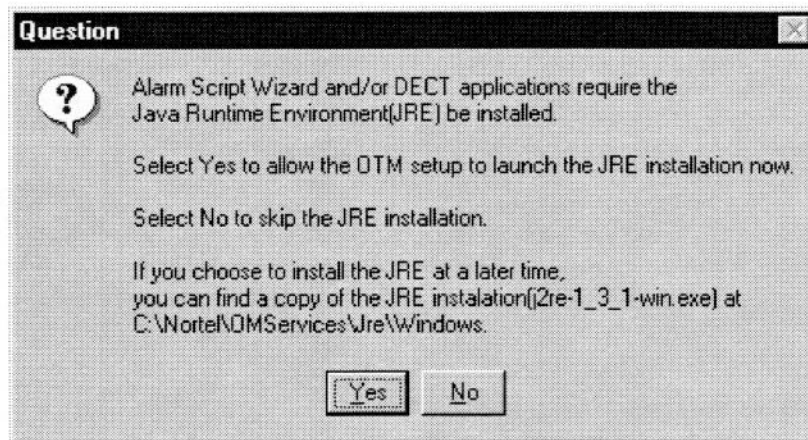
19 Click Yes to view the Read Me file or No to skip the Read Me file.

Java Runtime Environment

If you have installed applications that require Java* Runtime Environment (JRE), you are prompted to install JRE at this point (Figure 18).

20 Click Yes to install JRE.

Figure 18 JRE Installation



You may decide to install JRE at a later time. The JRE install program is located in the OTM directory (for example, C:\Nortel) at:

- For Windows: *C:\Nortel\NOMServices\Jre\Windows\j2re-1_3_1-win.exe*
- For other operating systems: Support for Java Plug-in Software on other operating systems is provided by the operating system vendor. For more information on Java Plug-in documentation and FAQ, refer to <http://java.sun.com/>.



Note: JRE is required for the Alarm Script Wizard and the DECT application.

System Restart

This dialog box asks you to restart the computer or end the installation without restarting the computer.

- 21** Select Yes, I want to restart my computer now, and then click OK.
- 22** Check the installation log to make sure you installed OTM software correctly, and that prerequisites have been met. During installation, the log resides in the following directory path: *C:\NortelLog\log.txt*. After installation, the log resides in the Local Data directory where you installed the application.

The OTM software installation is complete. The remaining sections in this chapter are:

- “OTM Client software installation” next
- “OTM upgrades” on page 64
- “Installing Web Help” on page 71
- “Migrating from MAT to OTM” on page 75



Note: You must run *Setup.exe* from your installation CD-ROM each time for the separate OTM install components: OTM and OTM Web Help.

OTM Client software installation

This section describes the OTM Client software installation. The installation steps are similar to the OTM Server installation. The steps are summarized below. See “OTM Server software installation” on page 41 to view the installation screens that are common to both procedures.



Note: Before installing OTM software, exit all Windows programs and disable any virus detection software.

- 1** Before installation:
 - a** Remove the MAT.exe shortcut file in the Start up folder, if present.

- b** On the OTM Server, share the Nortel directory with the specific users or User Groups that will be using the OTM Client.



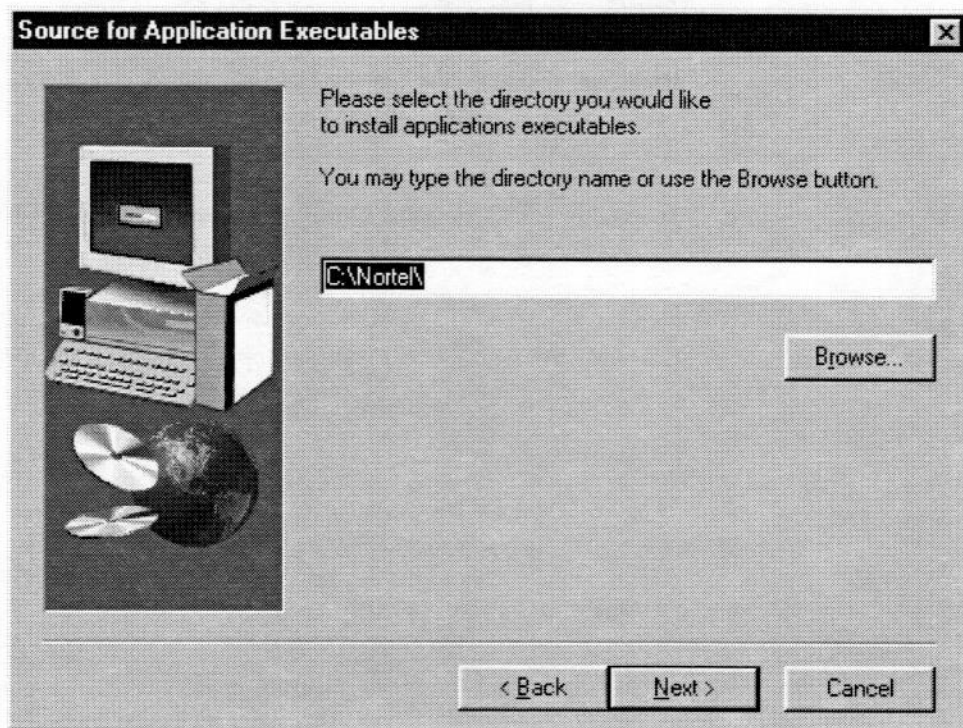
Warning: Assign share permissions for the Nortel directory according to your corporate security standards.

- c** On the Client PC, map the Nortel directory located on the OTM Server.
- 2** Double-click the *Setup.exe* file on the OTM CD-ROM.
 - 3** Navigate through the OTM installation wizard. The following screens appear (for examples, see “Software installation procedure” on page 43).
 - a** Welcome to the Software Installation Wizard
 - b** Software selection
 - c** OTM Software Licences Agreement
 - d** Welcome to the Optivity Telephony Manager Setup
 - e** Identification



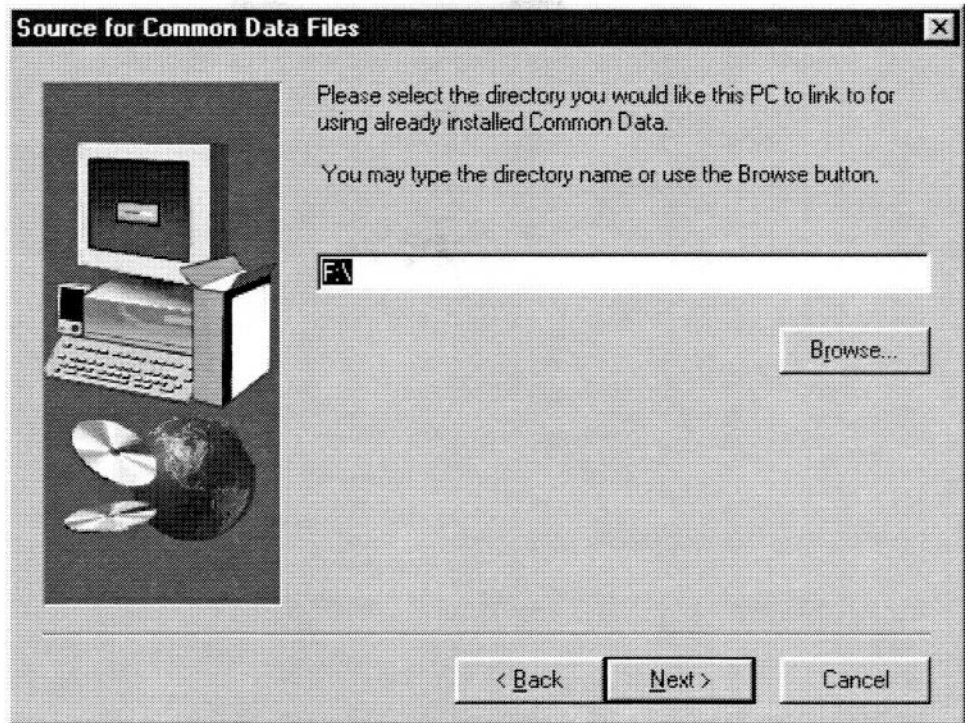
Note: If required, the setup program installs DCOM at this point if it is not present on the PC. Once installed, you must reboot the PC. After you reboot and log in, the OTM software installation continues.

- 4** In the Setup Choices dialog box, select Client.
- 5** Select the directory for the installation of the application executables as shown in Figure 19. Click Next to continue.

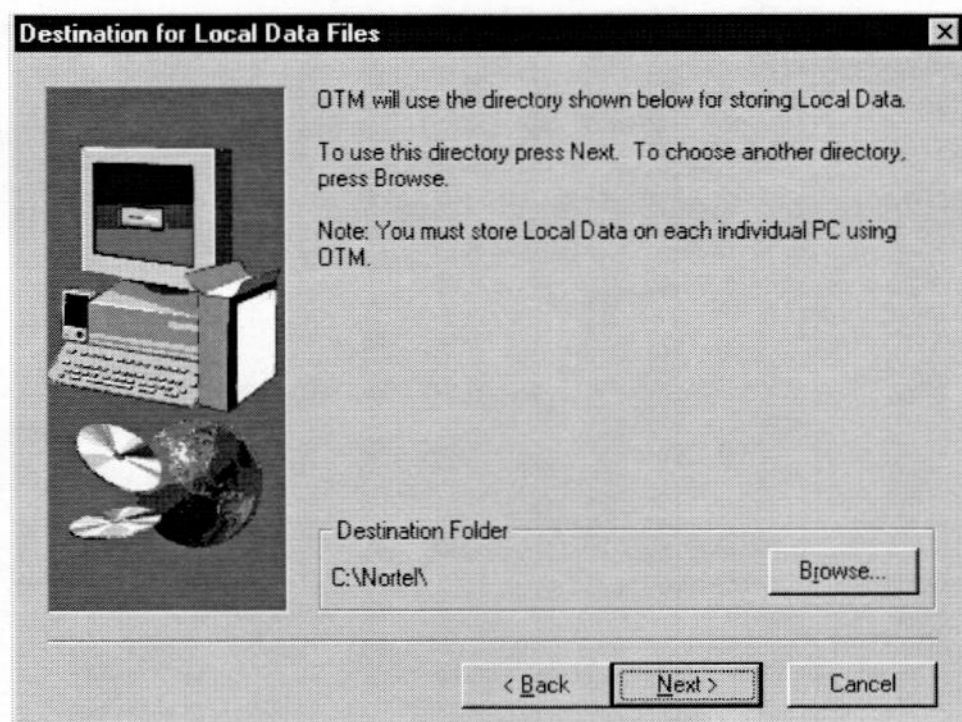
Figure 19 Source for Application Executables dialog box

Note: You may browse and select a local directory on the Client PC, or you may browse and select the mapped OTM Server directory.

- 6** Select the directory on the OTM Server where the Common Data files are stored as shown in Figure 20. Click Next to continue.

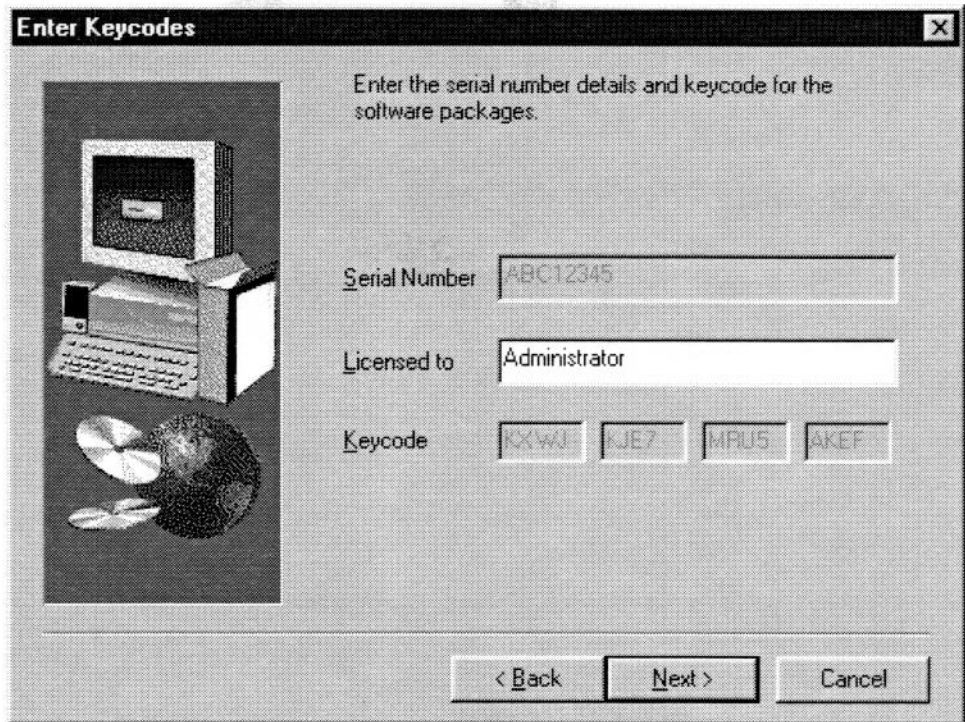
Figure 20 Source for Common Data Files dialog box

- 7 Select the destination on the Client PC for the local data files. See Figure 21. You must select a directory on the Client PC. Click Next to continue.

Figure 21 Destination for Local Data Files dialog box

Note: The setup program installs Microsoft Data Access Components (MDAC) at this point if it is not present on the PC. Once installed, you must reboot the PC.

- 8 The Enter Keycodes dialog box appears. See Figure 22. The fields contain the data stored on the OTM Server. Click Next to continue.

Figure 22 Enter Keycodes dialog box

The dialog box is titled "Enter Keycodes" and contains an illustration of a computer system and software discs on the left. The main area has a text label "Enter the serial number details and keycode for the software packages." followed by three input fields: "Serial Number" with the value "ABC12345", "Licensed to" with the value "Administrator", and "Keycode" with four buttons labeled "KXWJ", "KJE7", "MPUS", and "AKEF". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

Enter Keycodes

Enter the serial number details and keycode for the software packages.

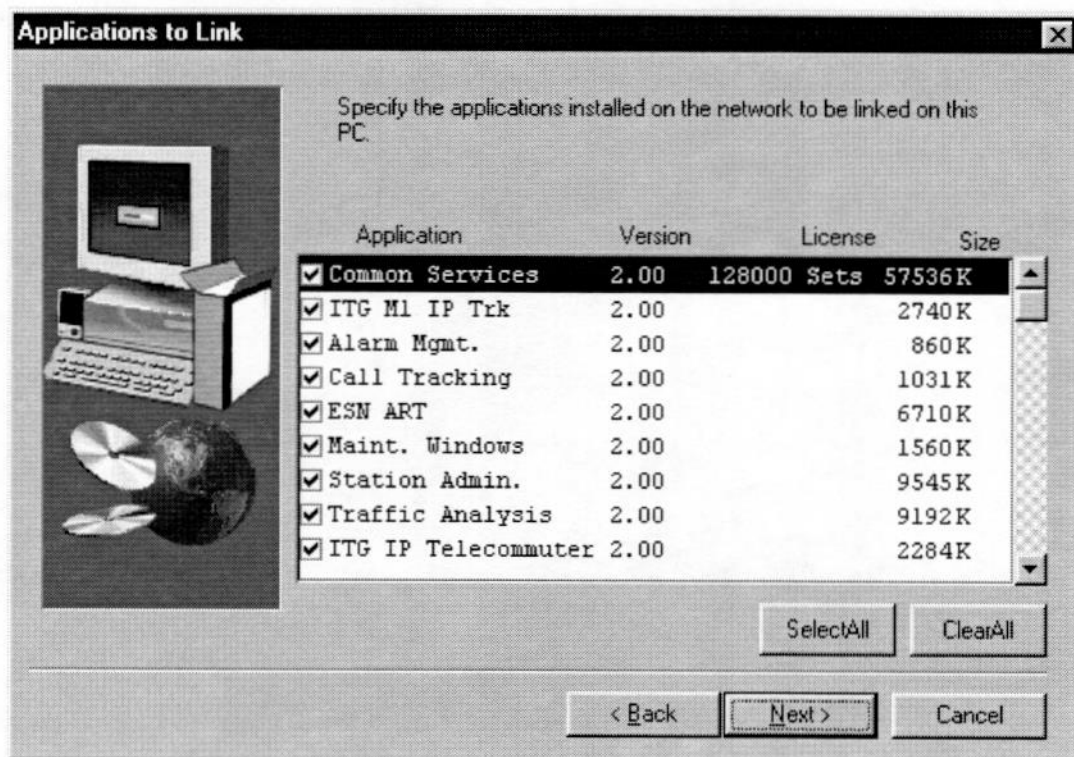
Serial Number: ABC12345

Licensed to: Administrator

Keycode: KXWJ KJE7 MPUS AKEF

< Back Next > Cancel

- 9 Select the applications to be installed if you chose to have the application executables installed on the Client PC, or select the applications to be linked if you chose to use the applications installed on the OTM Server. See Figure 23. Click Next to continue.

Figure 23 Applications to Link dialog box

- 10 The Applications to Install window appears (see Figure 16 on page 56). Click Next to continue.
- 11 After the installation is complete, you are given the option to view the Read Me file. Click Yes to view the Read Me file or No to skip the Read Me file.
- 12 When prompted, select Yes, I want to restart my computer now, and then click OK.

OTM upgrades

This section describes the various upgrade paths for OTM software.

Upgrading the OTM Server to the same release of OTM

You can upgrade the OTM Server for the following reasons:

- To install OTM applications not previously installed
- To upgrade to another OTM package (for example, from General to Premium)
- To increase the maximum number of OTM clients or the maximum number of sets (telephones) supported by OTM

The upgrade installation is very similar to the initial installation. You need a new keycode to upgrade to another OTM package or to increase the maximum number of OTM clients and sets (telephones).

Upgrading your OTM PCs

Upgrading from Windows 95

On an existing Windows 95 PC that is running OTM release 1.x, the OTM PC must first be upgraded to one of the supported PC platforms (See "OTM Server software requirements" on page 31) before upgrading the OTM software to release 2.0. To perform the upgrade, use the following procedure:

- 1 Perform a backup of the OTM data by selecting Utilities > Backup in the Navigator window. Choose the Disaster Recovery option.



Note: The following data is not backed up in OTM 1.x releases running on the Windows 95 platform:

- Alarm Notification Run Options parameters and Control/Script files
- Custom Help

- 2 Uninstall OTM 1.x.
- 3 Upgrade the PC to one of the platforms supported in OTM 2.0.
- 4 Reinstall OTM 1.x (the same release that was uninstalled in step 2).
- 5 Restore the OTM data by selecting Utilities > Restore in the Navigator window. Choose the backup file created in step 1.

6 Upgrade OTM to release 2.0.

Upgrading from Windows 98 or Windows NT

Before upgrading your PC, use the following procedure to upgrade OTM to release 2.0:

- 1 Upgrade OTM to release 2.0.
- 2 Perform a backup of the OTM data by selecting Utilities > Backup in the Navigator window. Choose the Full OTM Backup option.



Note: The following data is not backed up in OTM 2.0:

- Alarm Notification Run Options parameters and Control/Script files
 - Custom Help
-

- 3 Uninstall OTM 2.0.
- 4 Upgrade the PC to one of the platforms supported in OTM 2.0.
- 5 Reinstall OTM 2.0 (the same release that was uninstalled in step 3).
- 6 Restore the OTM data by selecting Utilities > Restore in the Navigator window. Choose the backup file created in step 2.



Note: When restoring users, if the user account no longer exists in the OS, then the user account will be created with the default password provided by the administrator during the restore process in step 6.

Upgrading to a new release of OTM

Perform this upgrade when installing a new release of OTM. Upgrade the OTM Server before performing OTM Windows Client upgrades.



Warning: Do *not* manually delete all the existing OTM program files when upgrading your system. If no OTM program files exist when you begin the Upgrade process, the system attempts to migrate your data from MAT to OTM. This causes a loss of data.



Note: If the client PC is a Windows 95/98 or Windows NT computer that is being upgraded to Windows 2000, delete any existing OTM directory and perform a fresh installation of the new version of OTM using the Server/Standalone option.

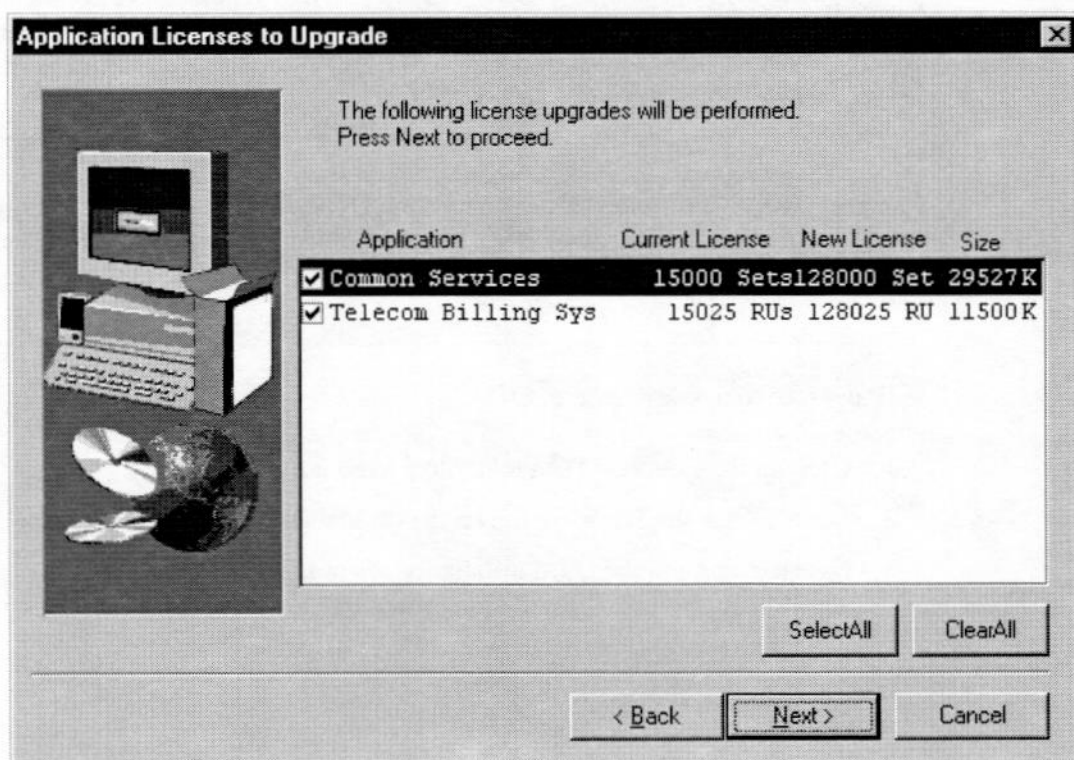


Note: If the client PC is an existing OTM client that is not being upgraded to Windows 2000, run an upgrade installation of OTM from the existing OTM server after the server has been upgraded to the new version of OTM.

To upgrade to a new release of OTM:

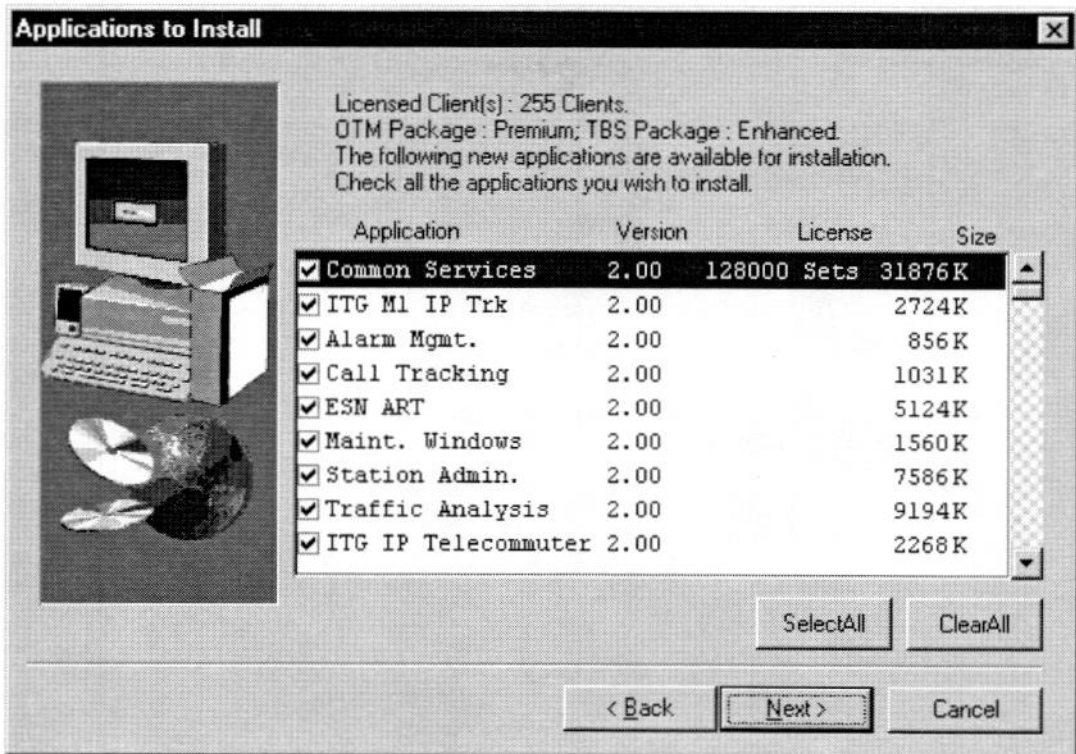
- 1 Back up the Common Data folder to a temporary directory.
- 2 Double-click the *Setup.exe* file on the OTM CD-ROM.
- 3 Navigate through the OTM installation wizard. The following windows appear (see “Software installation procedure” on page 43 for examples):
 - a Software Licences Agreement
 - b Welcome
 - c Identification
 - d Setup Choices. Select Server/Standalone to upgrade the OTM Server, or select Client to upgrade an OTM Client.
 - e Serial Number and Keycode
 - f Destination for files
 - g Application Licenses to Upgrade (Figure 24)

Figure 24 Application Licenses to Upgrade



h New Applications to Install (Figure 25)

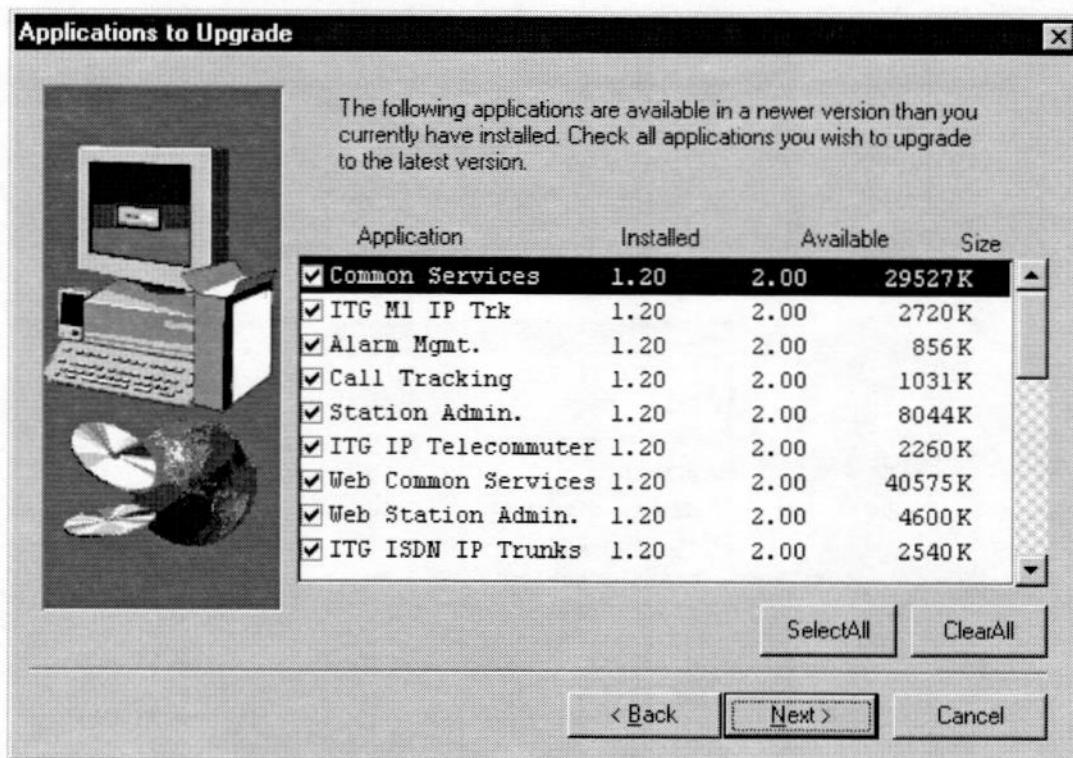
Figure 25 Applications to Install



i Applications to Upgrade (Figure 26)

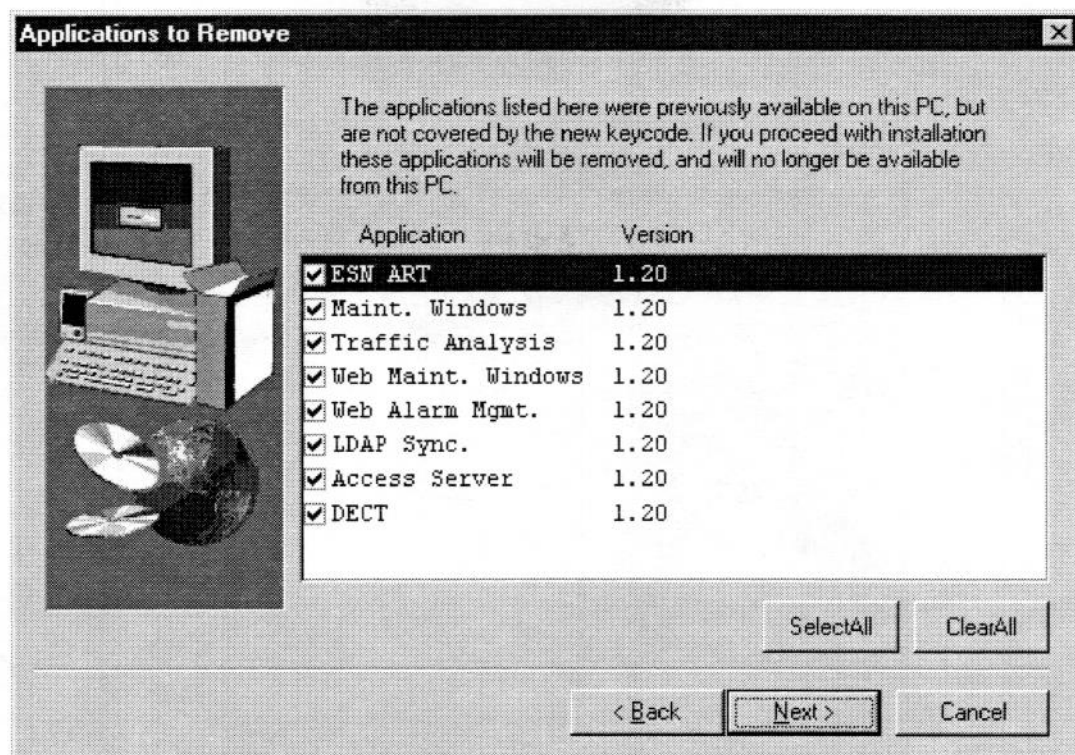


Note: When upgrading from an older release of OTM, you must choose to install the new versions of your existing applications. This is also a requirement when you are upgrading from the General or Enhanced package to the Enhanced or Premium package. If you do not install the new versions, the functionality provided in the new release of OTM will not be available.

Figure 26 Applications to Upgrade

- j Applications to Remove. These are applications available in the old keycode, but not available in the new keycode (Figure 27).

Figure 27 Applications to Remove



k Copying files

After the installation is complete you are given the option to:

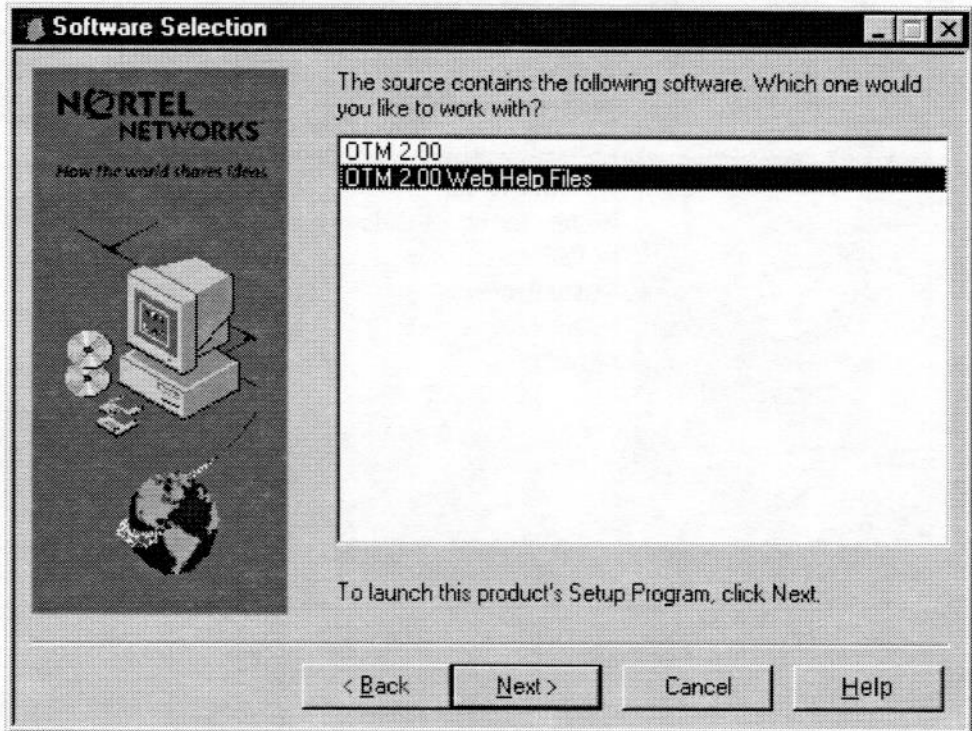
- 4 View the Read Me file.
- 5 Install JRE, if required.
- 6 Install OTM Web Help, if required.
- 7 Reboot the PC.

Installing Web Help

If you will be using OTM Web Services, install the Web-based Help files by selecting the option in the Software Selection dialog box (Figure 28).

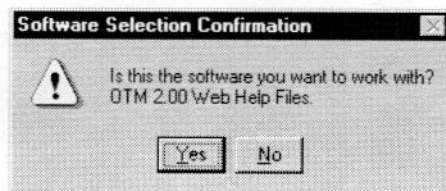
- 1 Double-click the *Setup.exe* file to launch the Software Installation Wizard (Figure 2 on page 44).
- 2 Select the OTM Web Help Files option, and then click Next (Figure 28).

Figure 28 Software Selection: Web Help



The Software Selection Confirmation dialog box (Figure 29) opens to request confirmation that OTM 2.00 Web Help Files is the software that you want to work with.

Figure 29 Confirmation Dialog Box

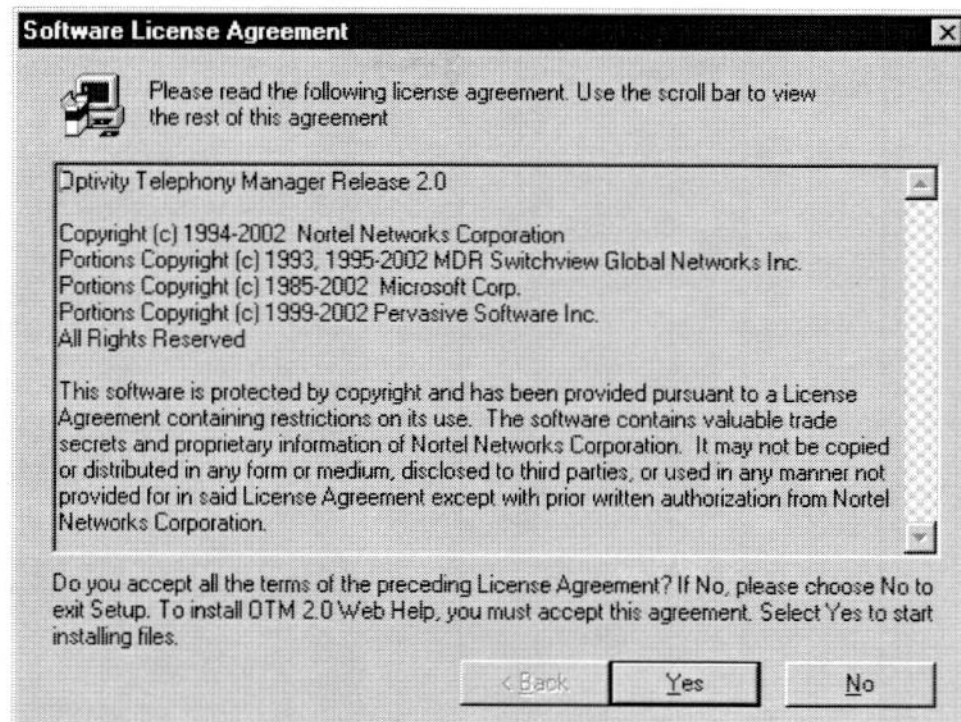


- 3 Click Yes to continue.

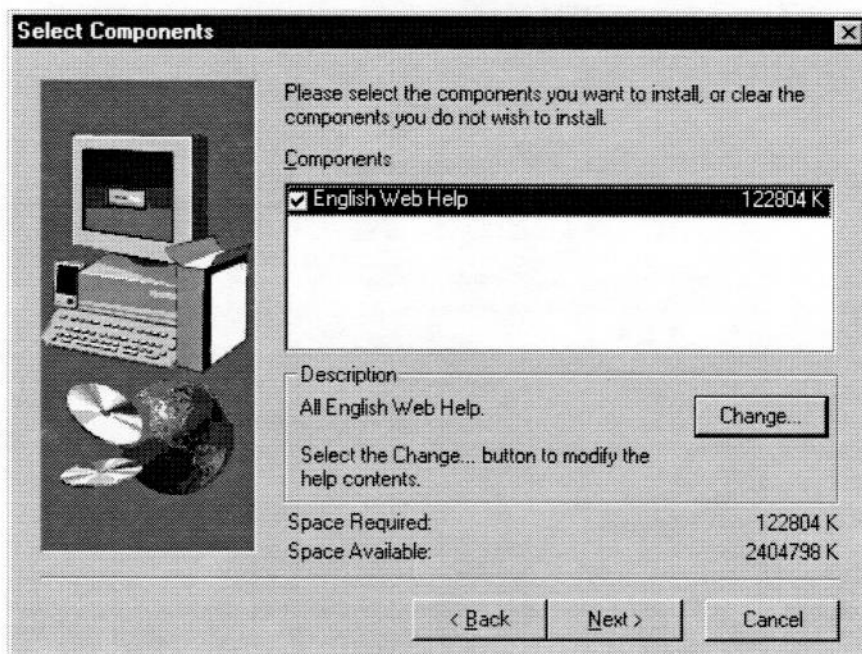
- 4 The "Software License Agreement" is the first dialog box displayed when you launch the OTM installation program (Figure 30). Click Yes to accept the agreement.

The Select Components dialog box appears (Figure 31).

Figure 30 Help License



- 5 In the Select Components dialog box, click Next to install all English Web Help, or click Change to select the sub-components that you want to install (Figure 32).
- 6 Click Continue in the Select Sub-components dialog box (Figure 32) to return to the Select Components dialog box (Figure 31).
- 7 Click Next to start the Web Help installation process.

Figure 31 Select Web Help components dialog box**Figure 32** Select Web Help sub-components dialog box

Migrating from MAT to OTM

Perform this upgrade when upgrading from MAT 6.6 or later to OTM. The migration copies and converts existing MAT data to the OTM PC. This data includes:

- MAT Site and System data
- MAT Users and Templates
- Application data (Station, ESN, and so on)



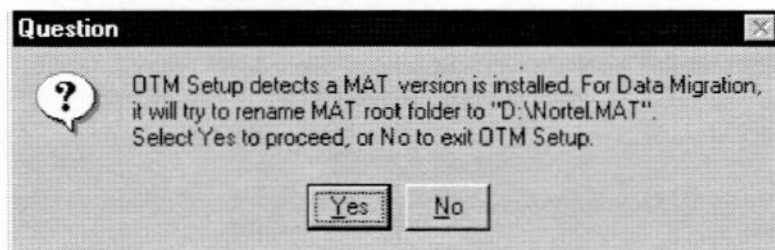
Note: Before upgrading to OTM, see “Migrating CDR data from MAT to OTM” on page 80 for information about transferring your Call Accounting data to OTM’s Telecom Billing System (TBS) application. You may also want to print your Call Accounting reports before upgrading from MAT to OTM.

There are four scenarios:

- 1 Installing OTM on a Windows 98/2000/NT Workstation on which MAT has been previously installed
- 2 Installing OTM on a Windows NT server being used as a MAT file server
- 3 Installing OTM on a clean Windows NT server and migrating the MAT data from another PC. See “Migrating data from MAT on one PC to OTM on another PC” on page 77.
- 4 Installing OTM on a MAT PC that is being upgraded to Windows 2000. See “Migrating data from MAT to OTM on a PC that is being upgraded to Windows 2000” on page 78.

Migrating data from MAT to OTM on the same PC

The migration is automatic if the setup program knows where MAT is installed (for example, installing OTM on a MAT PC) (Figure 33).

Figure 33 MAT Migration: OTM Setup dialog box

On the next reboot, run the MAT to OTM Migration tool to complete the migration process.



Note: Once the installation is complete and successful, you can delete the *Nortel.MAT* directory.

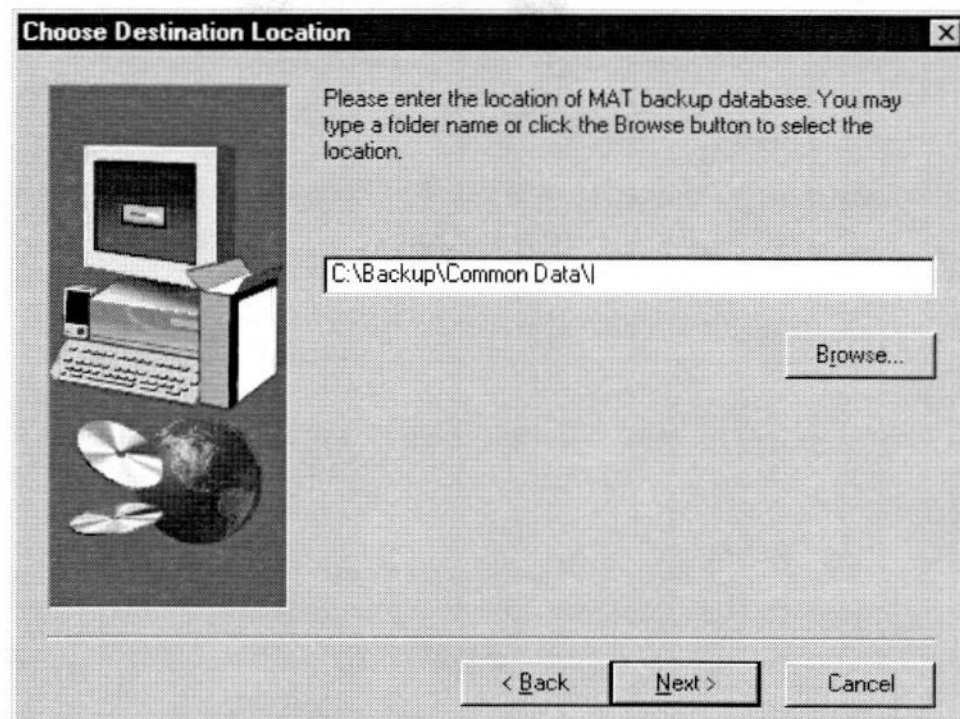
Installing OTM on a Windows NT server being used as a MAT file server

- 1 Back up the Common Data directory of MAT to a temporary directory:
 - a Create a new directory, such as *C:\Backup*.
 - b Copy the whole Common Data directory into *C:\Backup*. The backup data path is *C:\Backup\Common Data*.



Caution: To avoid loss of data, complete Step 1 first.

- 2 Install OTM.
- 3 Restart the PC.
- 4 In the Start menu, select Program Files > Optivity Telephony Manager > Database Migration Utility.
- 5 Run the utility.
- 6 When asked for the path to Common Data (to migrate), enter *C:\Backup\Common Data*, or click Browse and locate the backup directory (Figure 34).

Figure 34 MAT Backup Database: Choose Destination Location

- 7 When asked to make a selection to rebuild data, click Rebuild All.

Migrating data from MAT on one PC to OTM on another PC

- 1 Install OTM on the new PC.
- 2 Create a temporary directory on the OTM PC, such as *C:\Backup*.
- 3 Copy the Common Data directory on the MAT PC (typically located in *C:\Norte\Common Data*) to the temporary directory on the OTM PC (*C:\Backup\Common Data*).



Note: You can also copy the Common Data directory indirectly to the OTM PC by copying the Common Data Directory to a file server first.

- 4 On the OTM PC: In the Start menu, select Program Files > Optivity Telephony Manager > Database Migration Utility.

- 5 Run the utility.
- 6 When asked for the path to Common Data (to migrate), enter **C:\Backup\Common Data**.
- 7 When asked to make a selection to rebuild data, click Rebuild All.

Migrating data from MAT to OTM on a PC that is being upgraded to Windows 2000

On an existing Windows NT 4.0 server/workstation or a Windows 95/98 PC that is being upgraded to Windows 2000, use the following procedure:



Note: In this case, a current copy of MAT exists on the PC's hard drive.

- 1 Back up the Common Data folder to a temporary directory.
- 2 Uninstall MAT.
- 3 Upgrade the PC to Windows 2000.
- 4 Perform a fresh installation of OTM. See "OTM Server software installation" on page 41.
- 5 From the Start button, select Programs > Optivity Telephony Manager > Database Migration Utility. When asked for the location of the MAT database, type or browse to the location where the Common Data folder was backed up in step 1.



Note: For additional information on migrating the database from MAT to OTM, see "Migrating data from MAT to OTM on the same PC" on page 75.

Migrating data from MAT to OTM on a new Windows 2000 PC

On a new PC with Windows 2000 or an existing PC that has had its hard drive initialized before the installation of Windows 2000, use the following procedure:

- 1 Copy and rename the Nortel directory in the current copy of MAT.
- 2 Move the renamed Nortel directory to the Windows 2000 PC.
- 3 Perform a fresh installation of OTM on the new Windows 2000 PC. See "OTM Server software installation" on page 41.
- 4 Follow the procedure outlined in "Migrating data from MAT to OTM on the same PC" on page 75, beginning with step 4, to migrate the data from MAT to OTM.

MAT/OTM migration summary

Table 4 and Table 5 summarize the procedures for migrating data (from MAT to OTM). The migration procedures apply to the MAT version and OTM mode (such as Windows NT server or stand-alone) shown in each table.

Table 4 summarizes the migration steps to use OTM in Windows NT server mode. It also lists the MAT versions by target directory on the Windows NT system.

Table 4 Migration for OTM Windows NT server mode

MAT data migration for OTM Windows NT server mode:		
	Migrate data from MAT to OTM using same directory	Migrate data from MAT to OTM using different directory
Migration procedure on server	1. Move Common Data folder to c:/backup. 2. Run setup.exe on NT.	1. Run setup.exe on NT. 2. Run migration tool on NT.
Migration procedure on client	3. Run upgrade on client.	3. Run upgrade on client.
MAT Version to migrate		
6.6	95/98/WS/server	95/98/WS/server

Table 5 summarizes the migration steps to use OTM in stand-alone mode.

Table 5 Migration for OTM in stand-alone mode

	MAT data migration for OTM in stand-alone mode:	
	Migrate data from MAT to OTM on same computer	Migrate data from MAT to OTM on different computer
Summary of steps	Run setup.exe.	1. Run setup.exe. 2. Copy Common Data directory to c:/Backup. 3. Run migration tool.
MAT version to migrate		
6.6	95/98/WS/server	95/98/WS/server

Migrating CDR data from MAT to OTM

This section provides a procedure for migrating data from the MAT Call Accounting application to the OTM Telecom Billing System (TBS) application. The method outlined in this procedure takes advantage of the fact that the archived MAT Call Accounting data is in the same format as the data stored in an MDR 2000 buffer box.

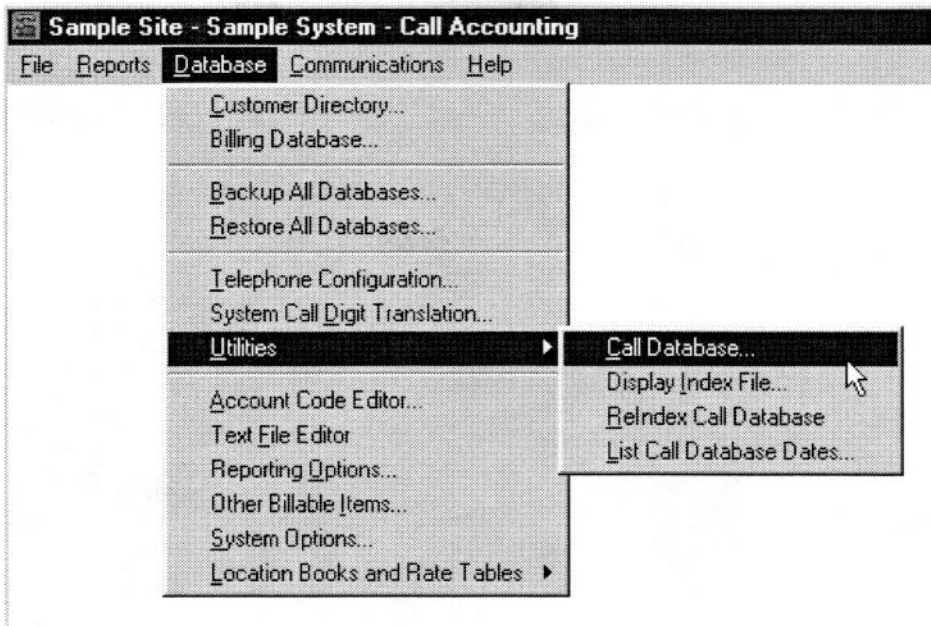


Warning: CDR and MAT Call Accounting data do not include the year in their date formats. TBS includes the year, which it retrieves from the CPU clock setting. If you use the procedure outlined in this section to migrate data from MAT to OTM, the data must be from the same year as the computer's current clock setting; otherwise, all data will be assigned the wrong year.

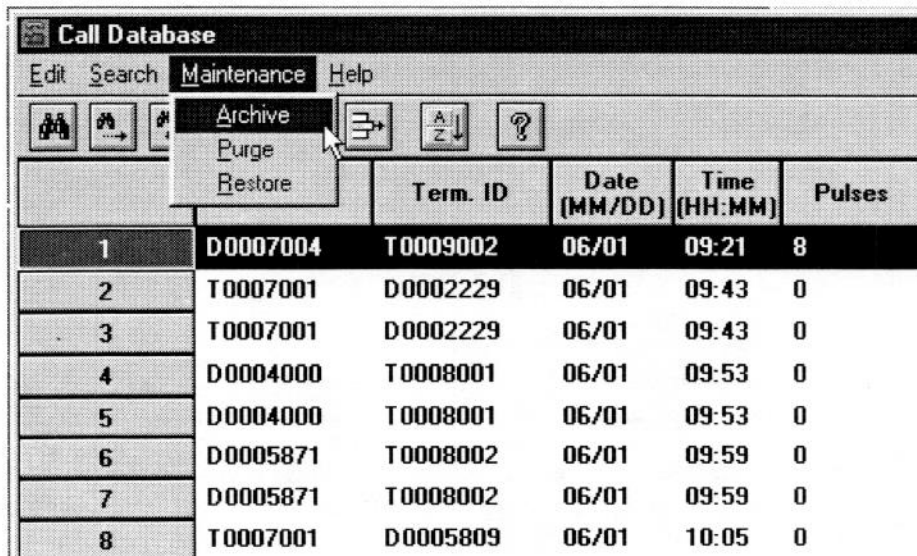
Before upgrading from MAT to OTM, you should archive your call data.

To archive call data:

- 1 From the Call Accounting application for the site/system, launch the Call Database (Figure 35).

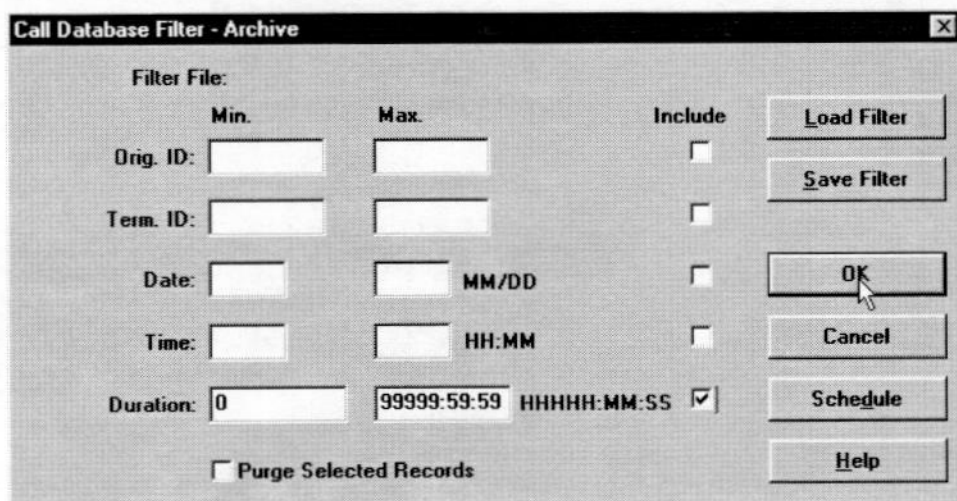
Figure 35 Launch Call Database

2 Select Archive from the Maintenance menu (Figure 36).

Figure 36 Launch Archive

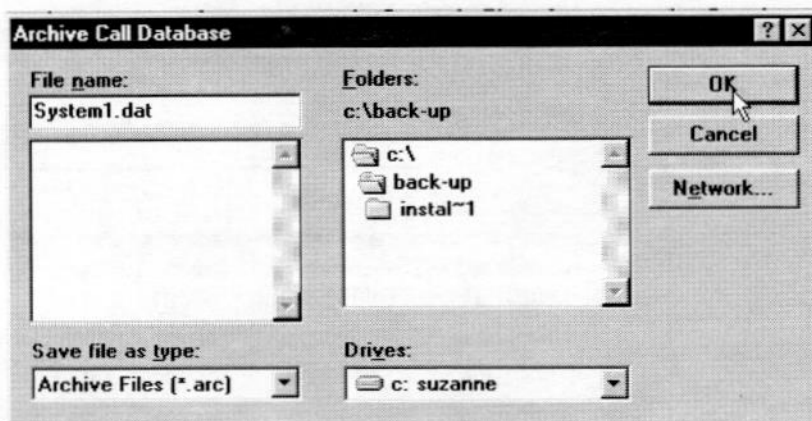
- 3 Enter an appropriate filter, and then click OK. All calls are selected in the example shown in Figure 37.

Figure 37 Archive Filter dialog box

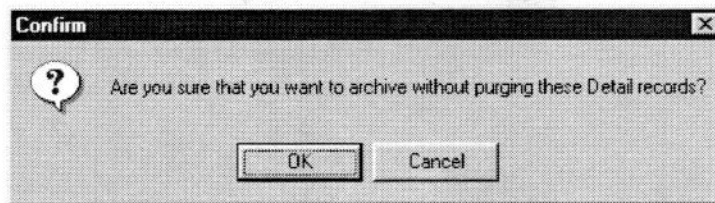


- 4 Name your file and choose where you want to save the file (Figure 38), and then click OK.

Figure 38 Store the Archive file



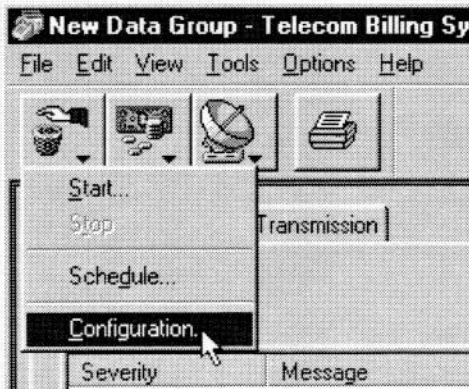
You can ignore the warning message (Figure 39). There is no reason to purge the data since the database will be obsolete after you upgrade from MAT to OTM.

Figure 39 Purge warning confirmation box

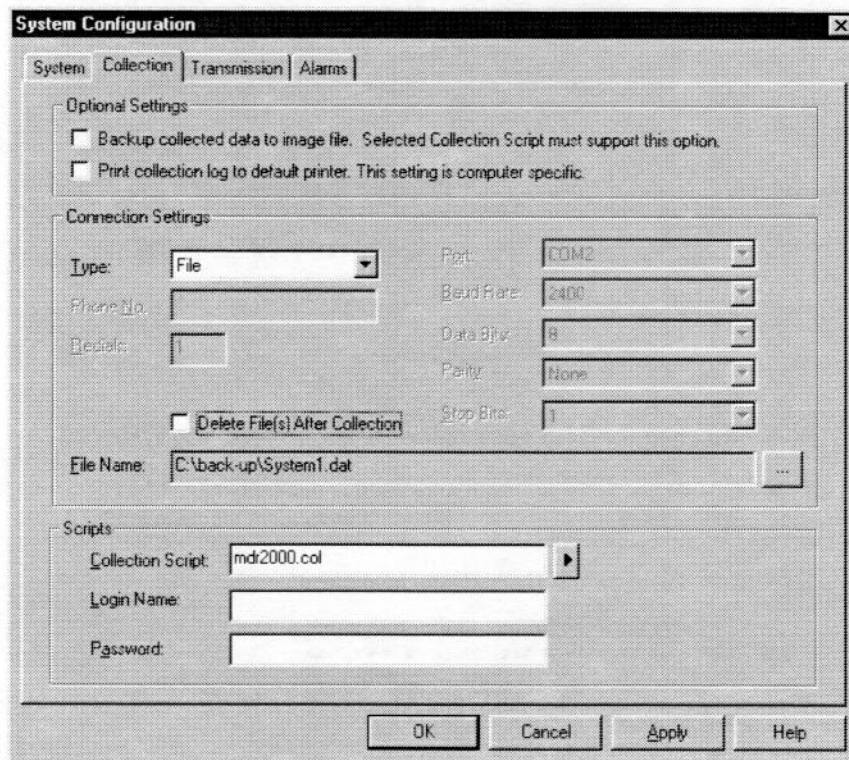
After you have upgraded from MAT to OTM, collect the archived Call Accounting data into the TBS application.

To collect the data into TBS:

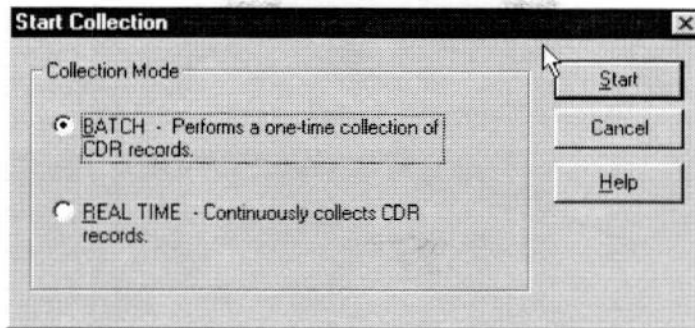
- 1 Launch the TBS application for the desired site/system.
- 2 From the TBS application, launch the Collection Configuration editor (Figure 40).

Figure 40 Launch Collection Configuration

The TBS System Configuration dialog box opens with the Collection tab selected (Figure 41).

Figure 41 TBS System Configuration—Collection tab

- 3** In the System Configuration—Collection dialog box:
 - a** Enter the File Name of the Call Accounting archive file. See step 4 on page 82.
 - b** For Collection Script, select *MDR2000.col*.
 - c** Uncheck the Delete File(s) After Collection check box to turn off the auto delete option.
 - d** Click OK.
- 4** In the Start Collection dialog box (Figure 42):
 - a** Select BATCH to collect the data in the Call Accounting archive file.
 - b** Click Start.

Figure 42 Start Collection dialog box

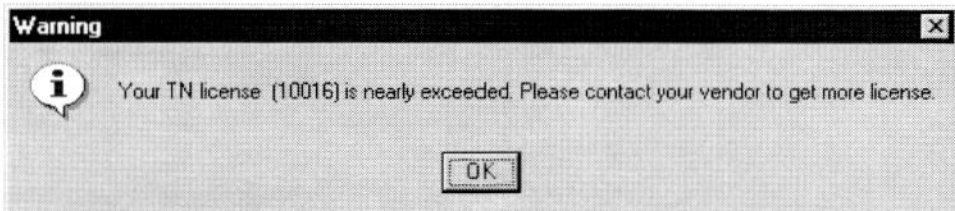
You can now use the normal TBS procedure to cost the CDR data. You will also want to modify your Collection Configuration to collect data from your site/system. See Chapter 2, "Telecom Billing System," in *Using Optivity Telephony Manager Telemanagement Applications* (553-3001-331) for information on TBS.

License management

The serial number and keycode, which you received with your OTM software package, determine the maximum number of terminal numbers (TNs), or telephones, reporting units (RUs), and OTM Clients that can be configured in your OTM system. To purchase licensing for additional TNs, RUs, or Clients, contact your OTM vendor.

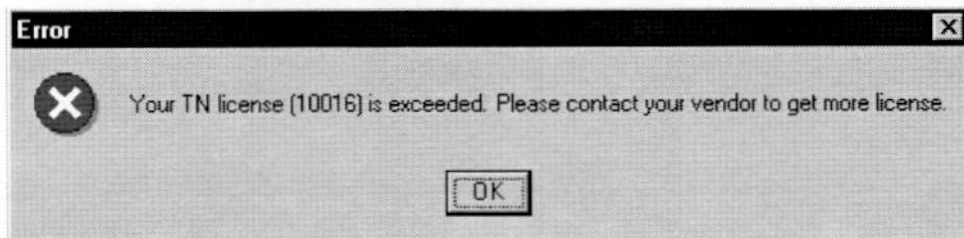
TN license

Each time you log in to OTM, your TN license is checked. If the number of set TNs (telephone TNs and virtual TNs) configured in your system is approaching the maximum for your license, the dialog box shown in Figure 43 appears.

Figure 43 TN license warning dialog box

If your TN license has been exceeded, the error message shown in Figure 44 appears. This message appears every 15 minutes. Contact your vendor to obtain a license for additional TNs.

Figure 44 TN license error dialog box



Note: TN checking is performed on bootup and after every 12 hours of operation. If you delete a site, the TN licenses associated with that site becomes available for reuse after the next TN check. If you are unable to wait for the next TN check, you can reboot the OTM server.

RU license

Reporting Units (RUs) are the base used for licensing the telemanagement applications in OTM. An RU represents a single entity in the OTM Corporate databases to which costs/usage can be assigned and reported on through the telemanagement applications. An entity can be either an employee in the Employee database, an external party in the External Parties database, or a role or project in the Roles/Projects database.

Each time you launch a telemanagement application in OTM, your RU license is checked. If the number of RUs configured in your system is approaching the maximum for your license, a warning dialog box appears.

If your RU license has been exceeded, you receive an error message. The TBS application continues to collect data; however, you cannot cost the data and generate reports. The GCAS application launches, but you cannot generate reports. Contact your vendor to obtain a license for additional RUs.

See *Using Optivity Telephony Manager Telemanagement Applications* (553-3001-331) for more information.

Client license

When you install an OTM Client, the host name of the OTM Client is registered on the OTM Server database. Each time a user attempts to log in to the OTM Client, the OTM software checks the OTM database. If the OTM Client is not located in the database, the dialog box shown in Figure 45 appears.

Figure 45 Client removed dialog box



This message appears if the OTM Client computer's host name has been changed or if the OTM Client has been removed from the OTM database.

If the host name of an OTM Client computer is changed, the OTM Administrator can use the Client Utility to update the host name in the OTM database. For information on the Client Utility, refer to *Using Optivity Telephony Manager* (553-3001-330).

Security device (dongle)

The process for checking the security device, commonly referred to as the "dongle," is different in OTM when compared to MAT. In MAT, every Client is required to have a dongle. In OTM, the dongle attached to the OTM Server allows access for all of the OTM Clients configured on the server.

When OTM is launched from an OTM Client, the OTM Server's dongle is checked. The OTM Client cannot launch the OTM System Window if the OTM Server's dongle is missing.

If the dongle has been removed from the OTM Server, it takes approximately 5 minutes, once it has been reattached, for the OTM Client to recognize the dongle.



Note: PCI-based parallel ports may have problems on certain operating systems. Compaq Proliant DL360R01 running Windows 2000 Server using a Lava PCI Bus Enhanced Parallel Port card is one such system. OTM does not support this configuration.

Chapter 2

Initial configuration tasks

After installing the OTM Server Software, follow the steps under “Logging in and changing the default password on Windows 98 stand-alone systems” on page 96 to connect to the Meridian 1 or Succession CSE 1000 system and change the default OTM password.

Test the connection using the sample site and system configuration. See “Testing the connection” on page 98.

After connecting successfully, refer to “Add sites and systems via the OTM Navigator window” on page 106 to configure your own sites and systems.

The complete list of OTM configuration procedures includes:

- “Configuring a modem for OTM applications in Windows” on page 90
- “Logging in and changing the default password on Windows 98 stand-alone systems” on page 96
- “Testing the connection” on page 98
- “Add sites and systems via the OTM Navigator window” on page 106
- “Add OTM Windows users via the OTM Windows Navigator” on page 151
- “Adding OTM Web Navigator users” on page 158
- “Setting Up the Meridian 1 or Succession CSE 1000 system” on page 180
- “Configuring Option 11C and Succession CSE 1000 systems for survivability” on page 190
- “Setting up virtual terminal service” on page 195
- “Setting up the Data Buffering and Access application” on page 200
- “Setting up the LDAP Server” on page 201
- “Setting Up Alarm Management” on page 202
- “Performing an OTM backup” on page 202
- “OTM Web browser Client installation” on page 204

- “Integrating OTM with Optivity NMS” on page 206
- “Integrating OTM with HP OpenView” on page 224

Configuring a modem for OTM applications in Windows

To ensure that a modem is configured correctly for use with Microsoft Windows 95, Windows 98, Windows 2000, or Windows NT Workstation 4.0, use the modem control panel to configure it. The modem control panel searches for and detects a connected modem automatically, and then stores the configuration information in the registry for other Windows applications to access.

The same is also true for OTM applications, where the modem configuration information is obtained by searching the Windows registry with the COM port specified in the communication profile. OTM communications software then sets up the Run-Time-Container (RTC) with the modem initialization string and communication profile settings for the application to make its connection to the Meridian 1 or Succession CSE 1000 system.

However, there are a number of limitations with this process that the user must take into account when configuring the modems:

- The Windows Modem control panel allows multiple modems to be configured on the same COM port.

OTM software always uses the first modem found in the registry configured for the specified COM port in the communications profile. To ensure proper modem operation, only one modem/communication device should be configured on a given COM port.

- A factory modem initialization (INIT) string is stored in the Windows registry. OTM applications use this INIT string to set up the modem connection.

The OTM communications software is written to use verbal (V1) result code. If the factory INIT string is set to use numeric (V0) result code, the “Can’t set modem parameters” error code occurs and the dial up attempt is aborted. To modify the factory INIT string, the user must use the registry editor (regedit) to change the factory INIT string to use verbal (V1) result code. See the Microsoft Windows documentation for detailed instructions on how to use the Registry Editor, or use the instructions below.

- When searching the modem configuration information in the Windows registry, the “AttachedTo” string value is used to identify which COM port is attached to the modem.

For a PCMCIA modem, this “AttachedTo” string value may not be available in the registry. As a result, no modem is found during the search and the RTC only contains the communication profile settings. To correct this problem, the user must use the registry editor (regedit) to add this “AttachedTo” string value of the COM port configured for the PCMCIA modem. See the Microsoft Windows documentation for detailed instructions on how to use the Registry Editor, or use the instructions below.

High-speed smart modem configuration consideration

As modem technology progresses, the new generation of high speed modems provide additional functionality to achieve the highest possible connection rate. These high speed smart modems use various tones during the handshaking period to negotiate the speed and protocol.

The modem configured on the Meridian 1 or Succession CSE 1000 SDI port is an area needing extra attention. In most cases, the modem attached to the SDI port is configured to run in dumb mode at the same speed for which the Meridian 1 or Succession CSE 1000 SDI port is configured (at 9600 bps or less). This locks the modem into a specific mode of operation preventing the modem from being run in command mode (echo input) or connecting at a different baud rate than what is configured for the Meridian 1 or Succession CSE 1000 SDI port.

When a high-speed smart modem is used on the OTM PC to dial up the Meridian 1 or Succession CSE 1000 modem, the PC modem always attempts to connect at its highest possible speed. The Meridian 1 or Succession CSE 1000 system’s modem, however, can only connect at the configured speed. Therefore, during the modem online handshaking period, the PC modem sends out different tones to negotiate the speed and protocol, and the switch modem connects at its configured speed and ignores additional attempts. Once the switch modem is connected, any additional handshaking tones sent by PC modem are translated into data (garbage under this condition) and forwarded to Meridian 1 or Succession CSE 1000 SDI port. These garbage characters may eventually lock up the Meridian 1 or Succession CSE 1000 SDI port. The two modems may still be connected, but access to the Meridian 1 or Succession CSE 1000 overlay input is no longer possible.

To avoid this type of problem, the key is to maintain modem compatibility. Here are some recommended steps to avoid potential problems and increase the connection success rate:

- The PC modem should be configured to match the switch modem's settings.
- The speed between the Meridian 1 or Succession CSE 1000 SDI port and Meridian 1 or Succession CSE 1000 system's modem is locked to the Meridian 1 or Succession CSE 1000 SDI port's baud rate if a high speed modem is installed on the SDI port.
- To minimize the garbage characters after carrier detect or carrier lost situations, set your modem S9 register to a higher value (for example, 30 = 3 seconds) and S10 register to a lower value (for example, 7 = 7/10 of a second).



Note: When increasing the value of the S9 register, you may need to do some timing adjustments on some of the modem/buffer equipment scripts.

Troubleshooting modem connections

Modem does not dial

Verify that your modem is configured on the correct COM port:

- 1 From the Start menu, select Settings > Control Panel.
- 2 Open the Modems file and click Properties.

Test the COM port to which your modem is connected by launching HyperTerminal:

- 1 From the Start menu, select Programs > Accessories > HyperTerminal.
HyperTerminal prompts you for a connection name and presents you with the phone number dialog box.
- 2 In the Connect Using drop-down list box, select Direct to COM X, where X is the COM port to which your modem is connected.
- 3 Once you are in the terminal, type the command AT.
The modem should respond with OK.

If your modem does not respond, you may be using the wrong COM port. To verify that you are using the correct COM port:

- 1 Go to the File/Properties menu and select Direct to COM *Y*, where *Y* is a different COM port.
- 2 Once you have located the correct COM port, go back to OTM Navigator and bring up the properties for the system to which you are trying to connect.
- 3 Click the communication tab, and then select PPP or Serial from the communication profile list.
- 4 Verify that the COM port you selected for this profile is the COM port on which you located your modem using HyperTerminal.
- 5 Verify that the baud rate matches the settings for the Meridian 1 or Succession CSE 1000 port into which you will dial.

If the modem still does not dial:

- 1 Follow the steps in the procedure "Test the COM port to which your modem is connected by launching HyperTerminal:" on page 92 to establish a HyperTerminal connection.
- 2 After issuing the **AT** command and receiving the OK prompt, issue the command **ATDT1234567**, where **1234567** is the phone number for the modem connected to the Meridian 1 or Succession CSE 1000 system.
- 3 Listen to determine whether the modem dials and connects:
 - a If you do not hear the modem dialing and connecting at this point, verify that your phone line and modem cables are connected correctly.
 - b If the modem dials and connects, verify that you have dial-up-networking installed along with a dial-up-adaptor.

Modem dials and connects but the connection details button reveals that scripting failed while waiting for a prompt

- ➔ In the Communications profile, verify that the baud rate configured for the TTY on the switch matches the baud rate configured for the modem in the PPP or Serial Communications profiles for the system to which you wish to connect. Make sure that the data bits, stop bits, and parity match as well.

To view the Communications profiles for a system:

- a** Right-click on the desired system in the Navigator window.
- b** Select Properties from the pop-up menu, and then click the Communications tab in the Properties dialog box.

Modem dials but does not connect

- 1** Verify that the phone number you are dialing is not busy.
- 2** Verify that you have included all necessary digits in the phone number.
- 3** Check the PPP or Serial Communications profiles for the system to which you wish to connect.

To view the Communications profiles for a system:

- a** Right-click on the desired system in the Navigator window.
- b** Select Properties from the pop-up menu, and then click the Communications tab in the Properties dialog box.

Modem dials and connects and the scripting is completed successfully, but the Connection Details button reveals that the session failed

- 1** Verify that the IP address that you assigned to the local PPP interface on the Meridian 1 or the Succession CSE 1000 is the same as the IP address you entered in the address field in the PPP Communications profile for the system to which you wish to connect.

To view the Communications profiles for a system:

- a** Right-click on the desired system in the Navigator window.
 - b** Select Properties from the pop up menu, and then click the Communications tab in the Properties dialog box.
- 2** If possible, verify that you can make an Ethernet connection to the same system:
 - a** After establishing a PPP connection, but before canceling the connection dialog, open a DOS command prompt: From the Start menu select Programs > MS-DOS Prompt
 - b** Run the ping command by typing `ping 47.1.1.10` where `47.1.1.10` is the Meridian 1 or Succession CSE 1000 system's local IP address. See "Setting Up the Meridian 1 or Succession CSE 1000 system"

on page 180 for information on configuring Ethernet and PPP on the Meridian 1 or the Succession CSE 1000.

- c Verify that the data lights on your modem flash as the ping data is sent to the Meridian 1 or Succession CSE 1000 system.



Note: If you do not receive a response from the Meridian 1 or Succession CSE 1000 system, verify that the IP address is the same as the one that you assigned to the local PPP interface on the Meridian 1 or Succession CSE 1000 system. To verify the IP address, go to the System Properties—Communication, PPP connection type dialog box, and confirm that the IP address that appears in the address field is correct.

Modem dials and connects but you receive the error message “Error writing to COM port” or “Error reading from COM port”.

- 1 Verify that the modem you installed in the Control Panel matches your modem type.
- 2 Remove your installed modem driver and install a generic modem driver in its place:
 - a From the Start menu, select Settings > Control Panel
 - b Double-click Modems.
 - c Click the Remove button to remove your modem from the installed list.
 - d Click Add to add a new modem driver.
 - e Click the check box that says “Don’t detect my modem; I will select it from a list”, and then click Next to move to the next step.
 - f Select the standard modem driver matching your modem’s baud rate (for example, Standard 28 800 bps Modem), and then click Next to move to the next step.
 - g Select the COM port to which your modem is connected, and then click Next.
 - h Click Finish to complete the modem installation.
 - i Restart the system, and try to establish a PPP or Serial connection.

Logging in and changing the default password on Windows 98 stand-alone systems

- 1 From the Start menu in the Windows Programs list, select Optivity Telephony Manager > Navigator.

In later sessions, OTM will automatically begin as part of the Windows start-up routine.



Note: The following information is applicable to Windows 98 stand-alone systems only. Windows NT and Windows 2000 users are authenticated using either a local account on the OTM Server, a Windows domain account, or LDAP. There is no default User ID and Password for these systems. See “Initial log in on Windows NT and Windows 2000 systems” on page 97 for information on logging in to non-Windows 98 systems.

- 2 Enter the default user ID and password shown below:

User ID: **ADMIN**

Password: **ADMIN**



Note: The password is case sensitive, and must be entered in all uppercase letters.



Note: For security purposes, the password does not appear as you type in the Password field.

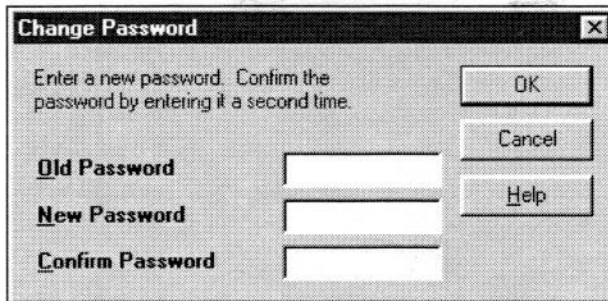
- 3 Click OK.

After OTM accepts your ID and password, the OTM Windows Navigator appears.

- 4 For Windows 98 stand-alone systems, change the default password to ensure security:

- In the Navigator window, choose Security > Change Password.

The Change Password dialog box appears (Figure 46).

Figure 46 Change Password dialog box

- Enter the old password in the Old Password field.
- Type a new password in the New Password field.
- Retype the new password in the Confirm Password field.
- Click OK.
- A message box informs you that the password was successfully changed. Click OK to close the message box.



Note: You must use this password the next time you start OTM.

When exiting from OTM, you are prompted to either log out of OTM or terminate OTM. If OTM is scheduled to complete any other tasks, such as Station Administration Synchronization, ESN, or Traffic, you should log out of the system but not terminate, as OTM continues to run in the background and complete the scheduled tasks.

Initial log in on Windows NT and Windows 2000 systems

Windows NT and Windows 2000 users are authenticated using either a local account on the OTM Server, a Windows domain account, or LDAP. There is no default Login Name and Password for these systems.

Any user account that is a member of the local Administrators group will always be able to log in to OTM, for example, Administrator. In a new OTM installation, use any local Administrators group account, Administrator for example, for your initial log in.

After logging in to OTM for the first time, you can set up additional users and user groups. To add user groups, select Security > User Groups from the OTM Navigator window, and then select Configuration > Add User Group... from the User Groups window. See “Creating a user group” on page 152 for detailed instructions on adding OTM user groups. To add users, select Security > Users from the OTM Navigator window, and then select Configuration > Add User... from the OTM Users window. See “Adding a user” on page 154 for detailed instructions on adding OTM users.



Note: Users that are not created from within OTM, Administrator for example, will not appear in the OTM Users window.

Testing the connection

Use the following procedures to test the connection between OTM and your equipment. For detailed instructions on adding sites and systems, see “Add sites and systems via the OTM Navigator window” on page 106.

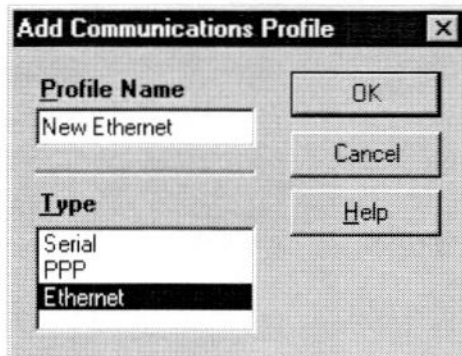


Note: The Embedded LAN (ELAN) must be configured and devices must be connected to the ELAN before you can test the connection.

Setting up communications information

- 1 Double-click Sample Site in the OTM Navigator window.
- 2 Click Sample System, and then choose File > Properties.
The System Properties dialog box appears with the General tab selected.
- 3 Click the Communications tab.
- 4 Click Add.

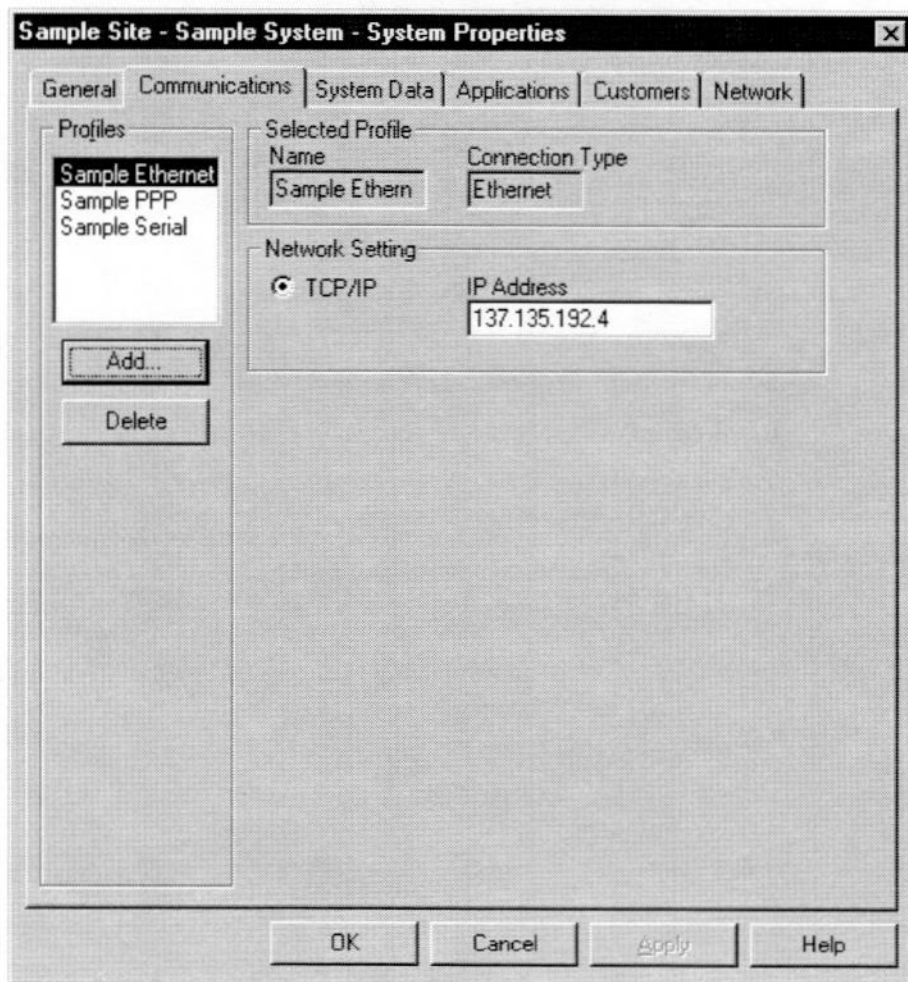
The Add Communications Profile dialog box appears (Figure 47).

Figure 47 Add Communications Profile dialog box

- 5 In the Type box, select a connection type that will be used by OTM.
- 6 Enter a Profile Name.
- 7 Click OK.
- 8 Enter the information in the System Properties—Communications dialog box for the connection type selected in step 5.

For an Ethernet connection type (Figure 48):

- a Enter the IP address that you configured on the Meridian 1 or Succession CSE 1000 system.
- b Click Apply.

Figure 48 System Properties dialog box—Communications tab—Ethernet Profile

For a PPP connection type (Figure 49):

- a Enter all modem parameters and dial-up information.
- b Select PPP in the Modem Script text box and enter the phone number.



Note: There may be conditions, depending on your particular installation, where you may be required to enter a Modem Access ID, a Modem Password, and a Modem Initialization String.

- c Set the IP address to the local IP address, as configured on the Meridian 1 or Succession CSE 1000 system.
- d Click Apply.

Figure 49 System Properties dialog box—Communications tab—PPP Profile

Sample Site - Sample System - System Properties

General | **Communications** | System Data | Applications | Customers | Network

Profiles

- Sample Ethernet
- Sample PPP**
- Sample Serial

Add...
Delete

Selected Profile

Name	Connection Type
Sample PPP	PPP

Port

CommPort: Com2

Connection Parameters

Data Rate	Stop Bits	Parity
9600	1 bit	None
Data Bits	Delay(secs)	Timeout(secs)
8 bits	0.500	30

System Access

Modem Script

Modem Script: PPP

Phone Number: 9555-1111

Modem Access ID:
Modem Password:
Modem Initialization String:

Network Setting

☒ TCP/IP

IP Address: 137.135.192.4

OK Cancel Apply Help

For a Serial connection type (Figure 50):

- a Enter all modem parameters and dial-up information.

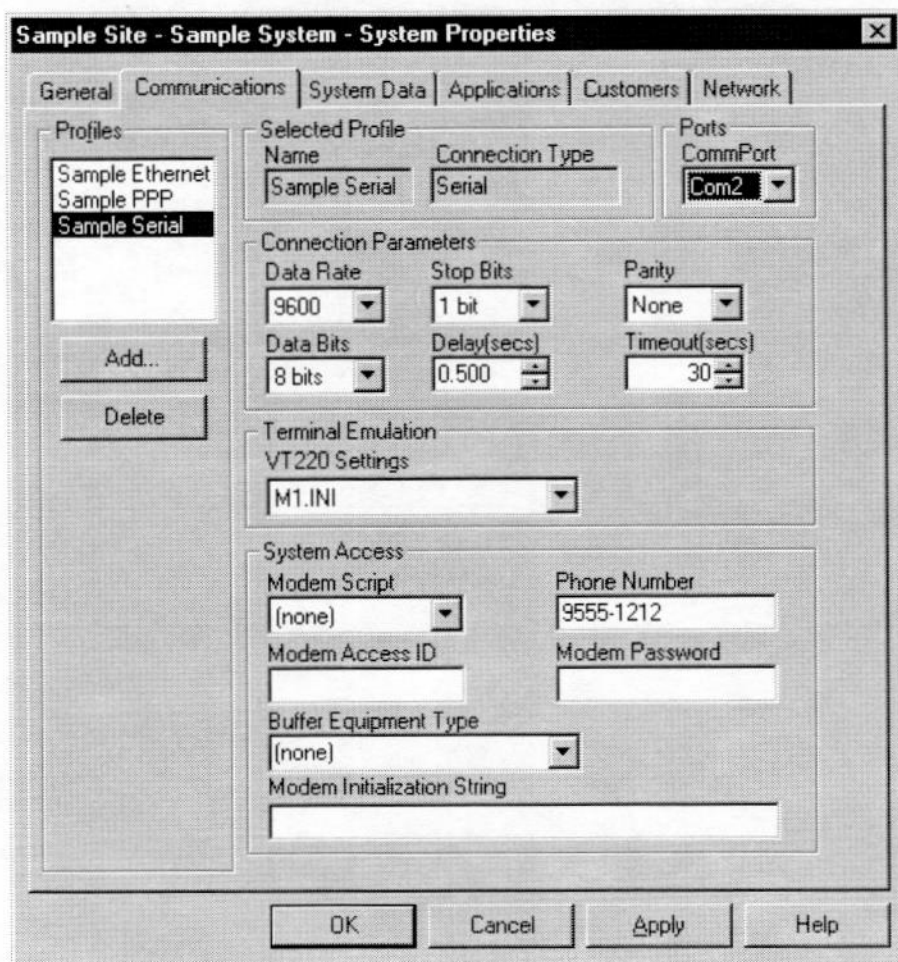
- b Select the appropriate value in the Modem Script text box.



Note: This is commonly “None” unless a specific value is defined for your system.

- c Click Apply.

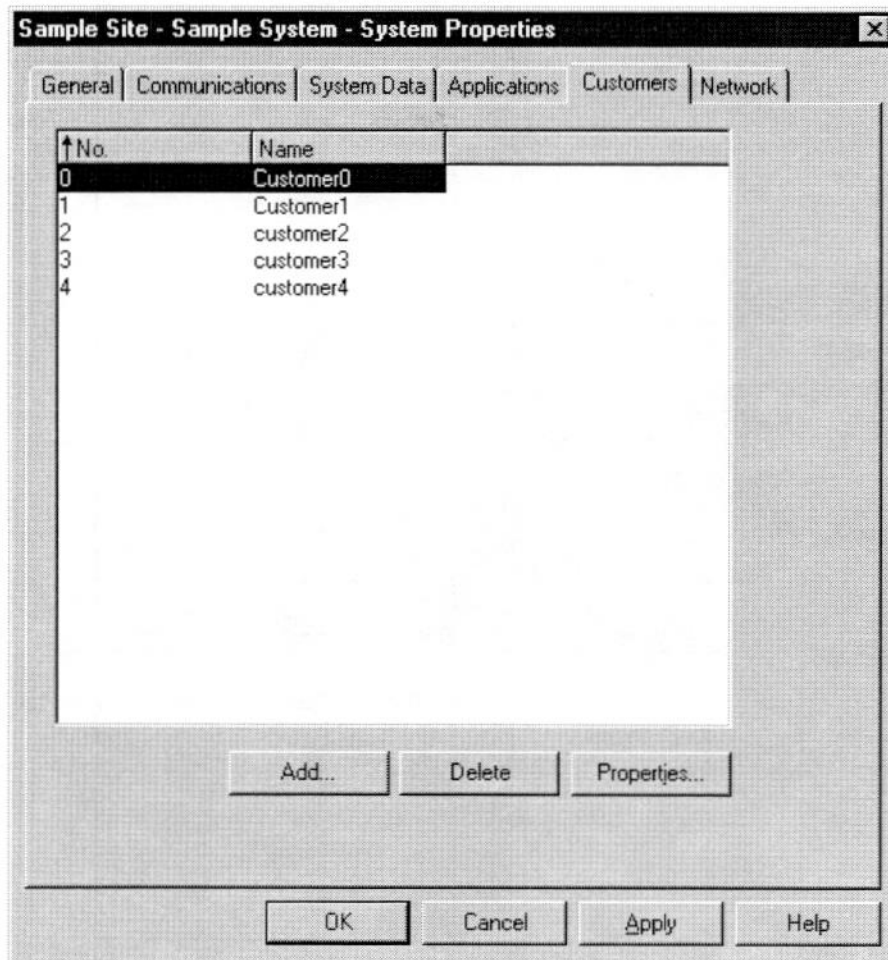
Figure 50 System Properties dialog box—Communications tab—Serial Profile



Setting up customer information

- 1 Click the Customers tab (Figure 51).

Figure 51 System Properties dialog box—Customers tab



- 2 Click the Properties button.

The Customer Properties dialog box appears with the General tab selected (Figure 52).

Figure 52 Customer Properties dialog box—General tab

Customer1 - (Customer 1) Properties

General | Features | Numbering Plans

Customer Name Customer1 **Number** 1

Directory Numbers

408-555-1212

HLOC 0

Scheduler System ID

User ID Maria

Password XXXX

OK Cancel Apply Help

- 3 In the Scheduler System ID box, change the User ID and Password to one that is valid for logging onto the Meridian 1 or Succession CSE 1000 system, and then click OK.



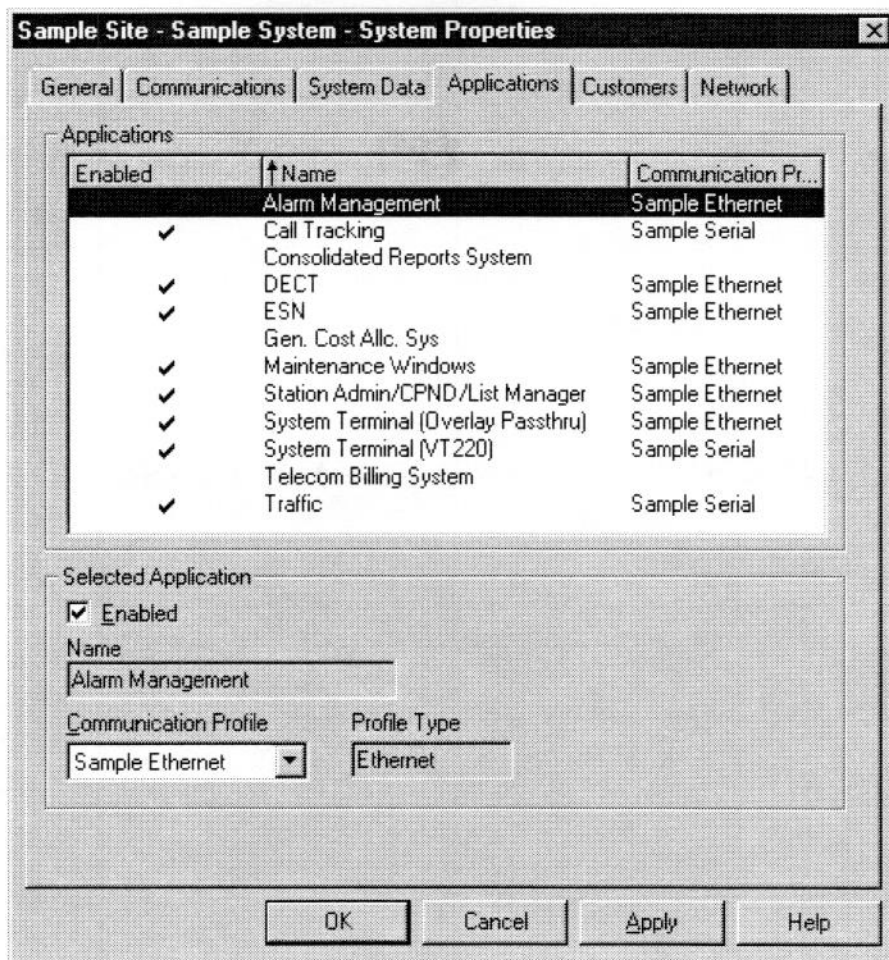
Note: HLOC displays the home location code (ESN) defined in LD90.

Setting up OTM applications

You must enable applications to make them available in the System window.

- 1 Click the Applications tab.

The System Properties dialog box—Applications tab appears (Figure 53).

Figure 53 System Properties dialog box—Applications tab**2** Enable each OTM Windows application:

- a** Select the application.
- b** Select a Communications Profile from the drop-down list box.

A check mark appears in the “Enabled” check box and next to the application name.

3 Click OK.

Setting up system data

- 1 Double-click the Sample System icon to open the System window.
- 2 Choose File > Update System Data.
- 3 Select the options **Update Data Stored in the PC** and **Do it Now**.
- 4 Click OK.

The system data (such as the PBX type and software packages) is copied into OTM directly from the Meridian 1 or Succession CSE 1000 system.

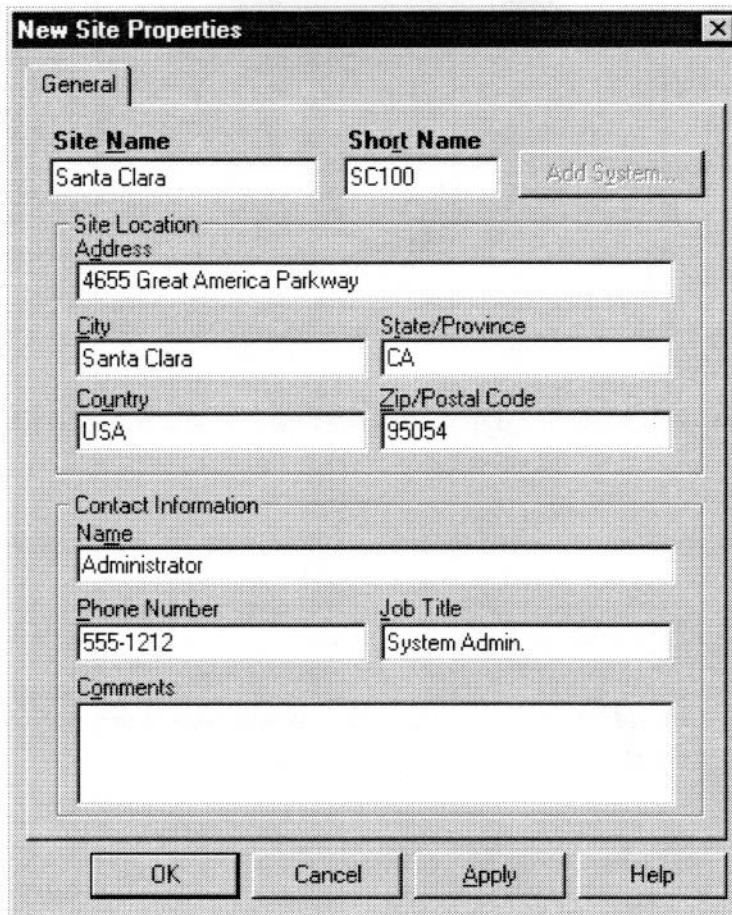
Once the data is copied from the system into OTM, the test procedure is complete.

Add sites and systems via the OTM Navigator window

Adding a site

You can add up to 3000 sites to the OTM Navigator window.

- 1 In the OTM Navigator window, choose Configuration > Add Site.
The New Site Properties dialog box appears (Figure 54).

Figure 54 New Site Properties dialog box

The image shows a 'New Site Properties' dialog box with a 'General' tab. It contains several input fields for site information. The 'Site Name' field is 'Santa Clara' and the 'Short Name' field is 'SC100'. There is an 'Add System...' button next to the 'Short Name' field. The 'Site Location' section includes an 'Address' field with '4655 Great America Parkway', a 'City' field with 'Santa Clara', a 'State/Province' field with 'CA', a 'Country' field with 'USA', and a 'Zip/Postal Code' field with '95054'. The 'Contact Information' section includes a 'Name' field with 'Administrator', a 'Phone Number' field with '555-1212', and a 'Job Title' field with 'System Admin.'. There is also a 'Comments' text area. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

New Site Properties	
General	
Site Name	Short Name
Santa Clara	SC100
Add System...	
Site Location	
Address	
4655 Great America Parkway	
City	State/Province
Santa Clara	CA
Country	Zip/Postal Code
USA	95054
Contact Information	
Name	
Administrator	
Phone Number	Job Title
555-1212	System Admin.
Comments	
OK	Cancel
Apply	Help

- 2 Fill in the Site Name and Short Name fields (these are required fields).
The Site Name appears in the Navigator tree. The Short Name is an abbreviated site name that displays in the Alarm Banner.
- 3 In the Site Location box, fill in the site address information.
- 4 In the Contact Information box, fill in the contact name and related information.
- 5 Click Apply.
- 6 To add a new system to this site:
 - a Click Add System.

- b** Follow the instructions for “Adding a Meridian 1 or Succession CSE 1000 Release 1.x system” on page 108, “Adding a Release 2.0 Succession CSE 1000 system” on page 127, or “Adding a Generic system or device” on page 148.
- 7** When you have finished entering Site information, click one of the following buttons to add the site to the Navigator tree:
 - OK adds the site and closes the property sheet.
 - Apply adds the site and leaves the property sheet open allowing you to add another system to this site. Repeat step 6 to add another system.
 - Cancel closes the dialog box without adding the site.

Adding a Meridian 1 or Succession CSE 1000 Release 1.x system

You can add as many as 256 systems (including non-Meridian 1 systems) to a site. You must have administrator privileges to add a system.

- 1** In the Navigator window, select the desired site.

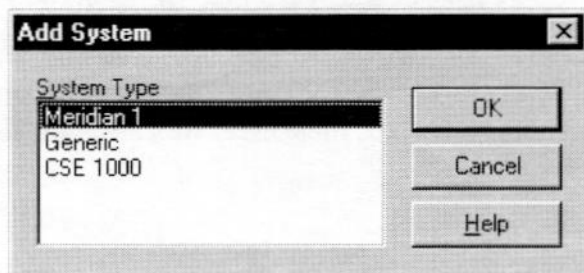


Note: If you are adding a new system from within the New Site Properties dialog box, skip to step 3 in this procedure.

- 2** Choose Configuration > Add System or use the right mouse button pop-up menu.

The Add System dialog box appears (Figure 55).

Figure 55 Add System dialog box—Meridian 1



- 3 In the Add System dialog box, select Meridian 1 and click OK.



Note: You must select Meridian 1 as the system type for Succession CSE 1000 systems prior to Succession CSE 1000 Release 2.0.



Note: You may need to install additional software to enable other system types not listed in Figure 55. Follow the installation instructions included with your order.

The System Properties dialog box appears with the General tab selected (Figure 56).

Figure 56 System Properties dialog box—General tab

Sample Site - Sample System - System Properties

General | Communications | System Data | Applications | Customers | Network

System Name **Short Name** **System Type**

Sample System SSM Meridian 1

System Location

☒ Same as Site

Address 2305 Mission College Blvd.

City Santa Clara State/Province CA

Country USA Zip/Postal Code 95052

Contact Information

☒ Same as Site

Name Administrator

Phone Number 555-1212 Job Title System Admin.

Comments

OK Cancel Apply Help

- 4 Enter the System Name and Short Name (required fields) and other information as needed. Click Apply.

You can make system location and contact information the same as site information by clicking the “Same as Site” check box.



Note: Bold fields indicate required information. To change a value, edit the field. Some fields may have a list of predefined choices. An arrow within a field indicates a drop-down list of choices. Press the arrow to select from the list. For more detailed information, refer to the online Help.

- 5 To add a new communications profile, click the System Properties dialog box—Communications tab.

This tab defines the types of communications profiles that may be applied to system applications (one profile may be used for multiple applications).

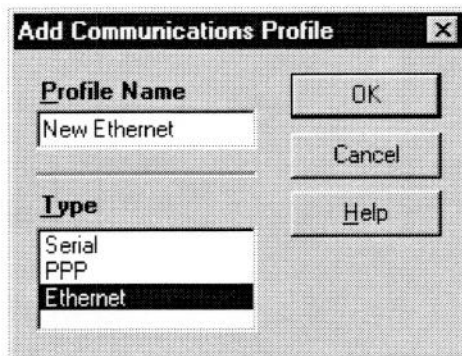


Note: OTM is shipped with a default communication profile. The Default profile is an Ethernet profile, and it cannot be deleted.

- 6 Click Add.

The Add Communications Profile dialog box appears (Figure 57).

Figure 57 Add Communications Profile dialog box

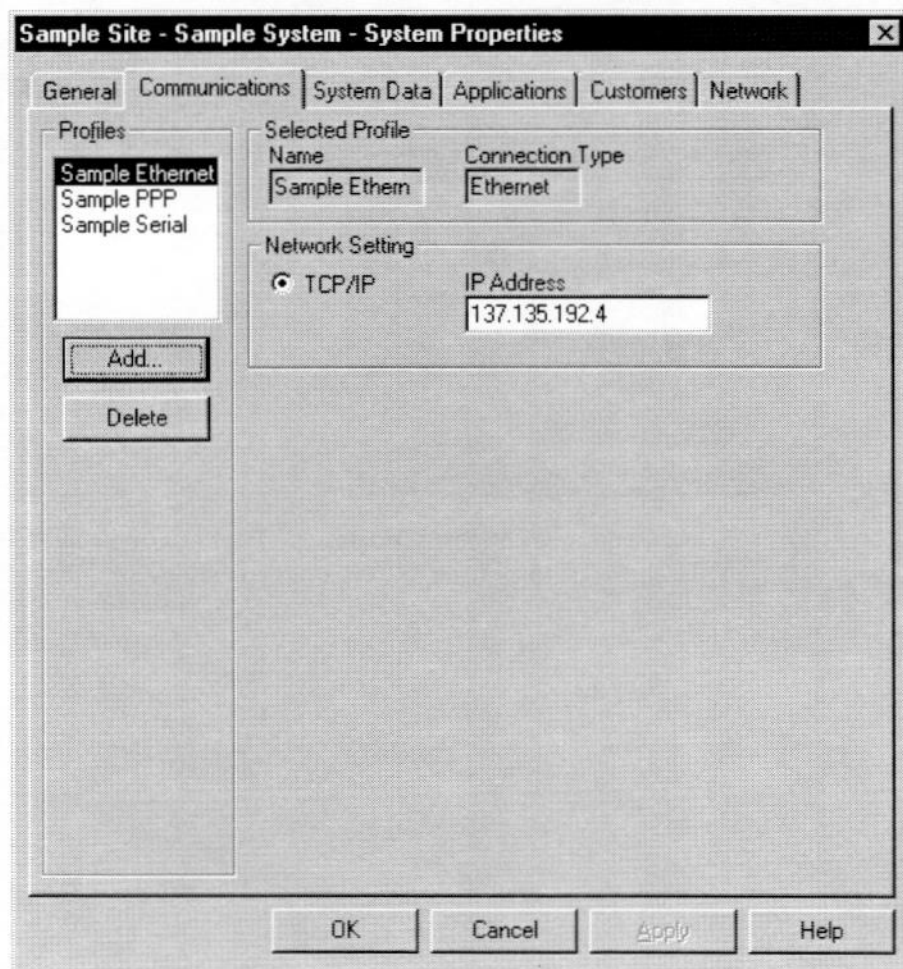


Select a communications type from the Type box and enter a Profile Name. Then click OK to go back to the Communications tab.

7 Fill in the communications information for the new profile:

- For Ethernet (Figure 58):
 - Select the appropriate network protocol.
 - Enter the IP address that you configured on the Meridian 1 or Succession CSE 1000 system.
 - Click Apply.

Figure 58 System Properties dialog box—Communications tab—Ethernet Profile



- For PPP (Figure 59):
 - Enter all modem parameters and dialup information.
 - Select PPP in the Modem Script text box.
 - Set the IP address to the local IP address, as configured on the Meridian 1 or Succession CSE 1000 system.
 - Click Apply.

Figure 59 System Properties dialog box—Communications tab—PPP Profile

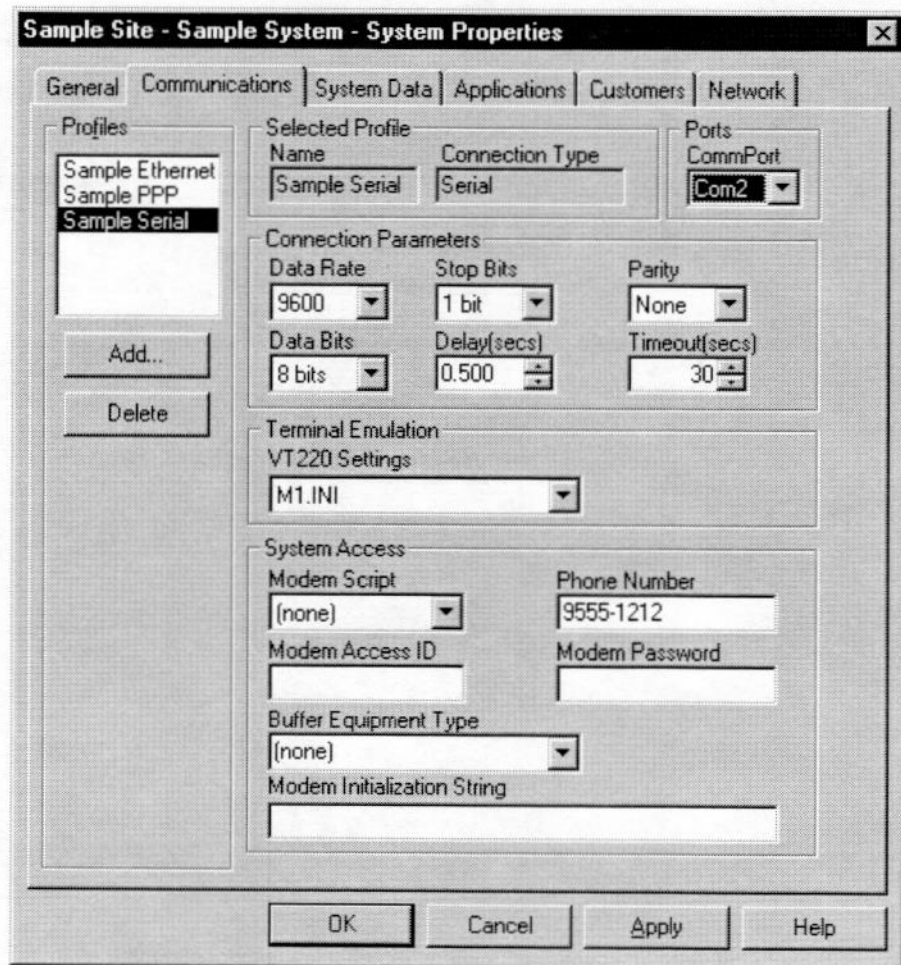
The screenshot shows the 'Sample Site - Sample System - System Properties' dialog box with the 'Communications' tab selected. The 'Profiles' list on the left includes 'Sample Ethernet', 'Sample PPP' (which is selected), and 'Sample Serial'. Below this list are 'Add...' and 'Delete' buttons. The main area is divided into several sections:

- Selected Profile:** A table with 'Name' as 'Sample PPP' and 'Connection Type' as 'PPP'.
- Port:** A dropdown menu showing 'Com2'.
- Connection Parameters:** A section with six fields: 'Data Rate' (9600), 'Stop Bits' (1 bit), 'Parity' (None), 'Data Bits' (8 bits), 'Delay(secs)' (0.500), and 'Timeout(secs)' (30).
- System Access:** A section with a 'Modem Script' dropdown set to 'PPP', a 'Phone Number' field with '9555-1111', a 'Modem Access ID' field, a 'Modem Password' field, and a 'Modem Initialization String' field.
- Network Setting:** A section with a radio button for 'TCP/IP' (which is selected) and an 'IP Address' field with '137.135.192.4'.

At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

- For Serial (Figure 60):
 - Enter all modem parameters and dial-up information.
 - Select the appropriate value in the Modem Script drop-down box. This is usually None unless a specific value is defined for your system.
 - Click Apply.

Figure 60 System Properties dialog box—Communications tab—Serial Profile



8 Click the System Data tab.

The System Properties dialog box—System Data tab appears (Figure 61). Enter the machine/system type and release version for the system, and enable or disable feature packages. For example, if your Meridian 1 is an Option 61C running X11 Release 25.25 software, use the drop-down boxes to select 61C in the Machine field and 25 in the Release field, and enter 25 in the Issue field. When you have finished entering the information in the System Data tab, click Apply.

Figure 61 System Properties dialog box—System Data tab

Sample Site - Sample System - System Properties

General | Communications | **System Data** | Applications | Customers | Network

Machine Information

Machine: **61C 060E** Release: **25**

Issue: **25** System ID: Cutover Date: **2/11/2000**

System Parameters

Maximum Speed Call Lists: **100** Maximum ACD Agents: **0**

☒ MARP allowed ☒ Multiple Loop DN

POI Password: **XXXXXXXXXX**

Packages

Enabled	Opt	Code	Description
	1	OPTF	Extended PBX Features
☒	2	CUST	Multi-Customer
☒	3	AIOD	Auto. Inden. of Out. Dial
☒	4	CDR	Call Detail Recording
☒	5	CTY	CDR - TTY
☒	6	CLNK	CDR - Mag. Tape
☒	7	RAN	Recorded Announceme
☒	8	TAD	Time and Date
☒	9	NNDI	Do Not Disturb-Indiv

Enable All **Disable All**

OK **Cancel** **Apply** **Help**



Note: For a Succession CSE 1000 Release 1.x system, select 11C as the machine type. Early versions of these systems are configured as Meridian 1 Option 11C systems, and their Media Gateways are configured as Survivable IP Expansion (SIPE) Cabinets.



Note: You can copy this data directly from an installed switch by scheduling an upload using File > Update System Data in the System window. Update System Data uses the communication profile for Station Administration. However, you should configure the Release number here first to allow available applications to show up properly in the Applications Tab.



Note: In the System Parameters box, the PDT Password edit box allows you to set the Level 2 password for the Problem Determination Tool (PDT). If you change this password, you must manually change the PDT password on the system so that they match.

9 Click the Applications tab.

The System Properties dialog box—Applications tab appears (Figure 62).

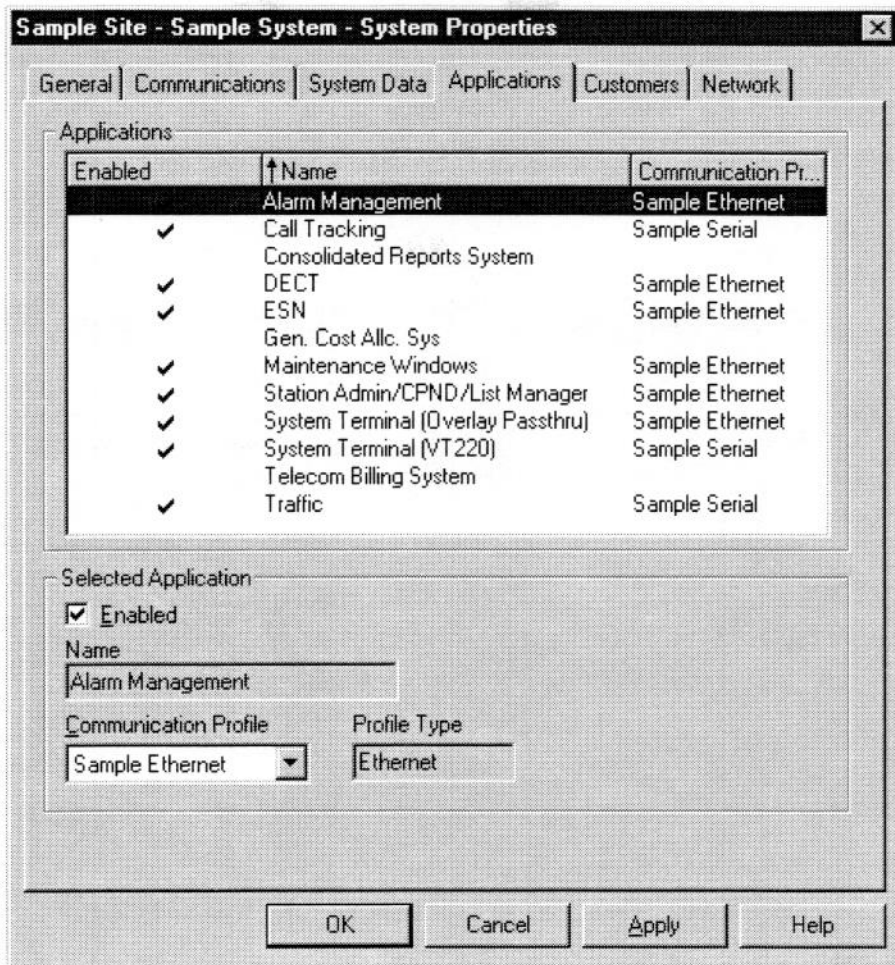
This tab defines the OTM applications that will appear in the System window and the communications profile to be used with each application.



Note: You must enable an application for it to be available in the System window.



Note: Communication profile settings are defined on a site/system basis and are shared by the OTM Server and its Clients. Consequently, if you define a serial communication profile for the Station Administration application, then both the OTM Server and OTM Client PCs must have a physical serial connection between the site/system and themselves. An OTM Client PC cannot use the COM ports of the OTM Server. Any communication task uses the resources of the PC on which it is running.

Figure 62 System Properties dialog box—Applications tab

To enable an application:

- a** Select the application in the Applications tab dialog box.
- b** Select a Communications Profile from the drop-down list in the Selected Application box.

A check mark appears next to the application, and the Enabled box is also checked.

To disable an application:

- a** Select the application in the Applications tab dialog box.

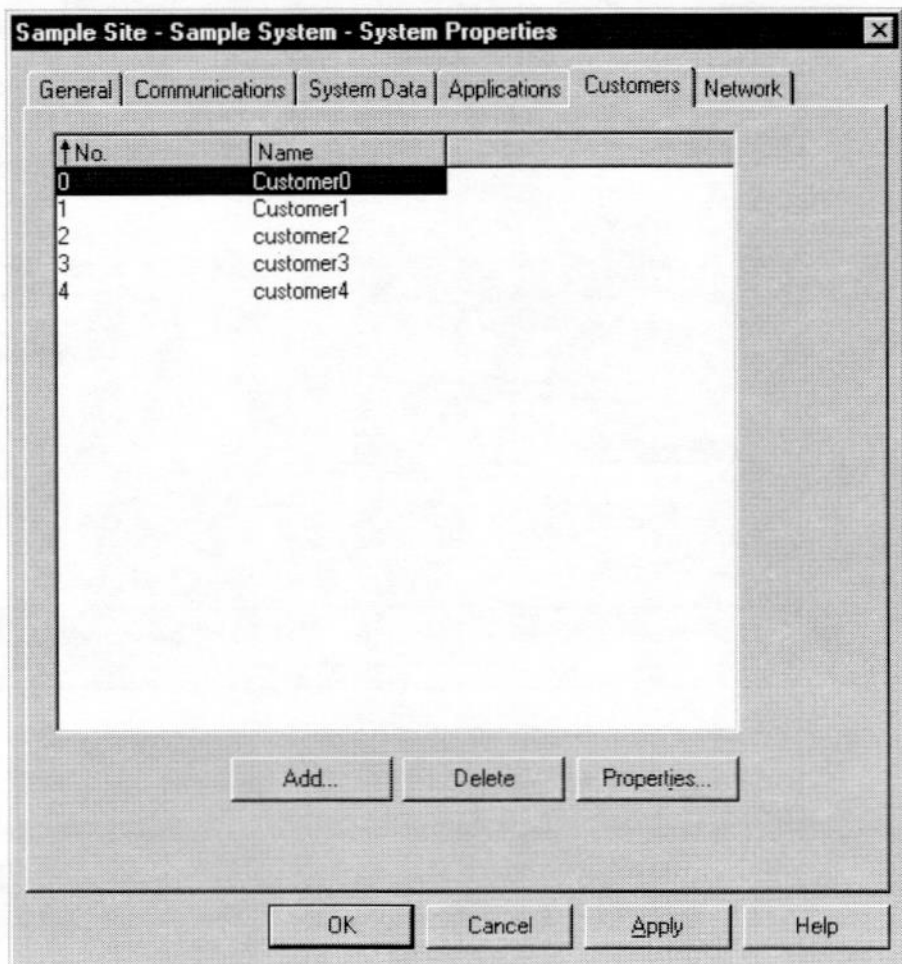
- b** In the Selected Application box, click the “Enabled” check box to remove the check mark.

When you have finished entering the information in the Applications tab, click Apply.

- 10** Click the Customers tab.

The System Properties dialog box—Customers tab appears (Figure 63).

Figure 63 System Properties dialog box—Customers tab



This tab lists the customers currently defined for this Meridian 1 system. You may add new customers, delete customers, or review the properties of a selected customer. When you add a new customer, you configure the Meridian 1 features and numbering plans that are available to the customer. This information is not automatically updated on the Meridian 1 system and must be updated by using the LD 15 customer overlay. LD 15 is the overlay interface that allows customers to configure their systems on the Meridian 1. For more information on overlay interfaces, see the System online Help.



Note: Customer information is required for System Administration/CPND and ESN applications.

11 To add a customer:

- a** Click Add in the System Properties dialog box—Customers tab.
- b** Select a Customer number.
- c** Click OK.

The Customer Properties dialog box appears with the General tab selected (Figure 64).

Figure 64 Customer Properties dialog box—General tab

Customer1 - (Customer 1) Properties

General | Features | Numbering Plans

Customer Name **Number**

Directory Numbers

HLOC

Scheduler System ID

User ID
Password

OK Cancel Apply Help

- d** Fill in the general information for the customer.



Note: You can copy this data directly from an installed switch by scheduling an upload using File > Update System Data in the System window. Update System Data uses the communication profile for Station Administration. However, you should configure the Release number here first to allow available applications to show up properly in the Applications Tab.

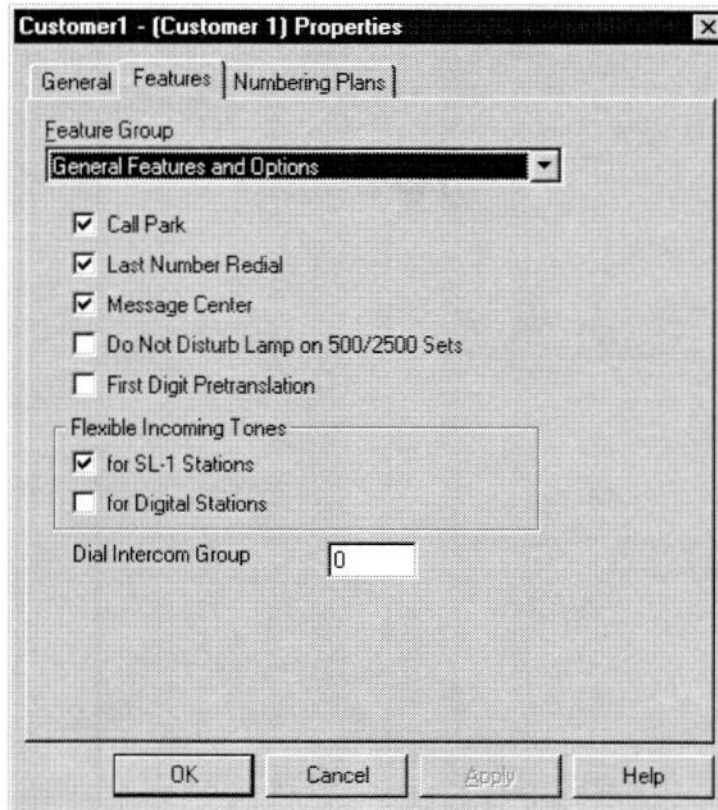


Note: Enter User information in the Scheduler System ID text box if you are using applications with scheduled activities, such as Station Administration/CPND, ESN, and Traffic Analysis.

- e** Click the Features tab.

The Features dialog box appears (Figure 65).

Figure 65 Customer Properties dialog box—Features tab



f Fill in the feature information for the customer.

g Click the Numbering Plans tab.

The Numbering Plans dialog box appears (Figure 66).

Figure 66 Customer Properties dialog box—Numbering Plans tab

Customer1 - (Customer 1) Properties

General | Features | **Numbering Plans**

DID	DN Type	from	to
	ACD DN	3000	3499
	ACD Position ID	3500	3999
✓	Regular DN	4000	4500

Selected Line

DN Type [dropdown] [Add]

Range: from [text] **to** [text] [Delete]

☐ Direct Inward Dial

Exchange [text] [dropdown]

Usage [text]

Access Code Type :

[OK] [Cancel] [Apply] [Help]

h Fill in the numbering plan information for the customer.

- 12** When you have finished entering the customer information, click one of the following buttons to save the information:
 - OK adds the customer and returns you to the System properties sheet.
 - Cancel closes the dialog box without adding the customer.
 - Apply adds the customer and leaves the Customer properties open so that you can add other information for this customer.
- 13** To delete a customer, click Delete in the System Properties dialog box—Customers tab. A delete confirmation box appears. Click OK.
- 14** To modify customer information, click Properties in the System Properties dialog box—Customers tab. The Customer Properties dialog box appears with the General tab selected. Modify information in the appropriate tabs and click OK.

15 Click the Network tab.

The System Properties dialog box—Network tab appears (Figure 67).



Note: The Network tab is used to both add and delete Survivable IP Expansion Cabinets and Survivable Media Gateways. On Meridian 1 systems, all SurvivableIP Expansion Cabinets must be deleted before the main Meridian 1 system can be deleted.

Figure 67 System Properties dialog box—Network tab

Sample Site - Sample Option 11C - System Properties

General | Communications | System Data | Applications | Customers | Network

Select the Gatekeeper Zone to which this switch belongs. Typically, this is only done when the PBX has a Gatekeeper compatible ITG node.

Zone: Sample Zone Edit

Sample Zone
West Coast

Survivable Carbinets

Site	System	Cabinet Number	Address
SC3	SC1	1	47.22.33.1
SC4	SC3	2	47.22.34.5
SC5	SC7	3	47.22.36.11

Add Edit Delete

OK Cancel Apply Help

- a If the system is a Succession CSE 1000 Release 1.x system or a Meridian 1 with a Gatekeeper-compatible ITG Trunk node, select the Gatekeeper Zone from the drop-down list.



Note: If the system does not contain a Gatekeeper-compatible ITG Trunk node and you continue, you add the system to a Gatekeeper Zone for display in the OTM Windows and Web Navigators only.

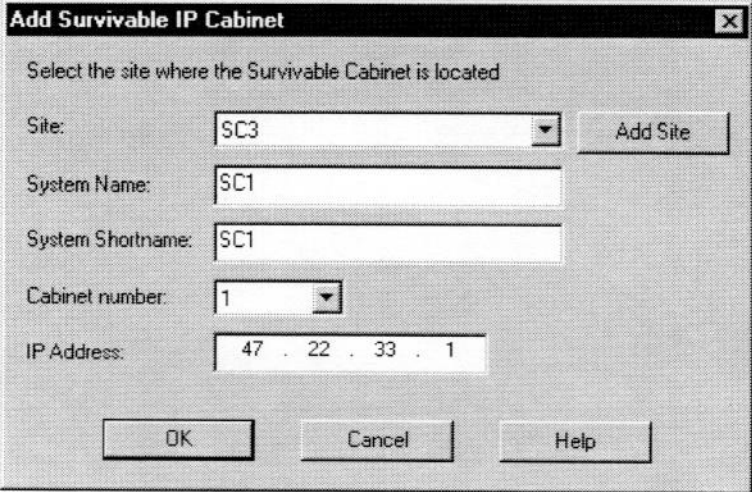


Note: For information on managing gatekeeper zones, see “Managing gatekeeper zones” on page 146.

- b If the system is not a Succession CSE 1000 Release 1.x system with Survivable Media Gateways or a Meridian 1 Option 11C with Survivable IP Expansion cabinets, go to step 16.
- c If the system is Succession CSE 1000 Release 1.x system or a Meridian 1 Option 11C that is being configured to support Survivable IP Expansion cabinets or Media Gateways, click Add to add a cabinet.

The Add Survivable IP Cabinet dialog box appears (Figure 68).

Figure 68 Add Survivable IP Cabinet dialog box



The dialog box is titled "Add Survivable IP Cabinet". It contains the following fields and controls:

- Select the site where the Survivable Cabinet is located** (instructional text)
- Site:** A drop-down menu showing "SC3". To its right is an "Add Site" button.
- System Name:** A text field containing "SC1".
- System Shortname:** A text field containing "SC1".
- Cabinet number:** A drop-down menu showing "1".
- IP Address:** A text field containing "47 . 22 . 33 . 1".
- At the bottom are three buttons: "OK", "Cancel", and "Help".

- d Select the Site and Cabinet number from the drop-down lists, and enter the System Name, System Shortname, and IP address for this cabinet.

For additional information on Option 11C survivable expansion cabinets, see *Option 11C Planning and Installation* (553-3021-210).

For additional information on the Succession CSE 1000 Media Gateway, see *Succession Communication Server for Enterprise 1000 Planning and Installation* (553-3023-210).

- e** Click OK.

A new System Properties dialog box appears.



Note: The Applications tab settings are copied from the Main Cabinet system properties. If the *Default* Ethernet communication profile is selected for the applications on the Main Cabinet that are likely to be used by the Survivable IP Expansion Cabinets, you can click OK to add the SIPE Cabinet and return to the System Properties dialog box—Network tab for the Main Cabinet (step 15b).

- f** Enter the requested information for the General and Communications tabs (see steps 4 through 7 in this procedure).

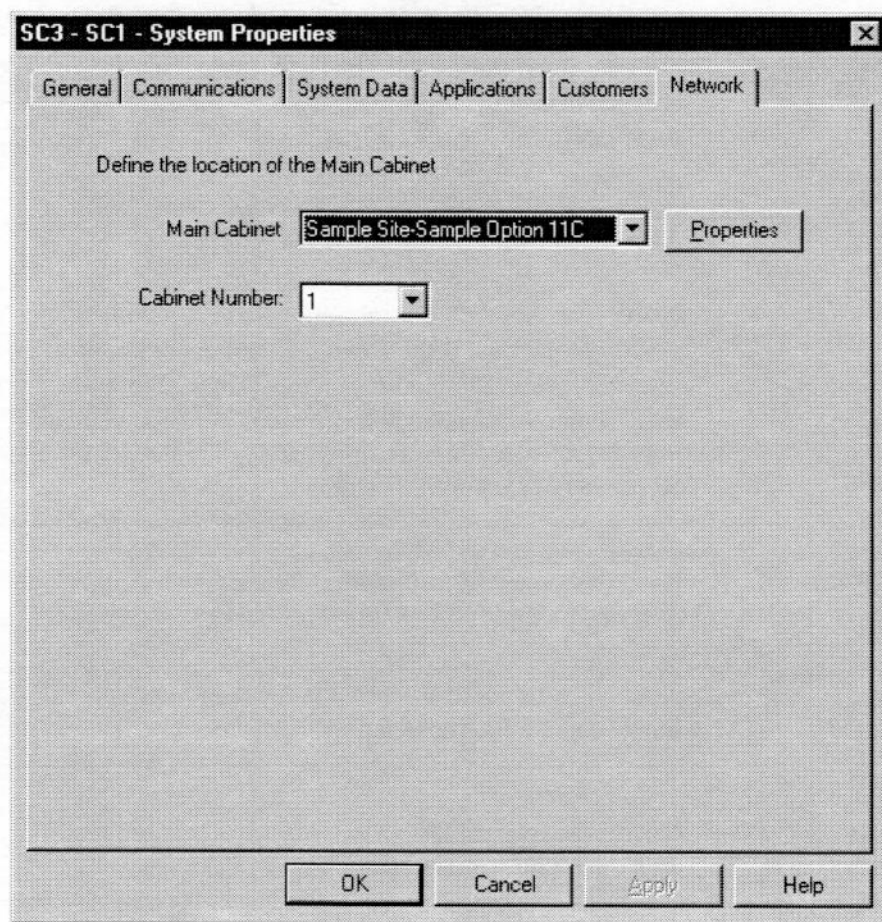


Note: The IP address entered in the Add Survivable IP Cabinet dialog box is copied into the default Ethernet communication profile.



Note: The System Data and Customers tabs are read-only. These contain the information from the main cabinet.

- g** Click the Network tab. The System Properties dialog box—Network tab appears (Figure 69).

Figure 69 Survivable Cabinet System Properties dialog box—Network tab

- h** Select the Main Cabinet and the Cabinet Number from the drop-down lists.
 - i** Click OK to close the System Properties dialog box for the Survivable IP Expansion cabinet and return to the System Properties dialog box—Network tab for the Main Cabinet.
- 16** In the System Properties dialog box, click one of the following buttons:
- OK adds the system and closes the dialog box.
 - Cancel closes the dialog box without adding the system.
 - Apply adds the system and leaves the dialog box open.
 - Help provides online Help.

The new system is added to the tree under the selected site.

Adding a Release 2.0 Succession CSE 1000 system



Note: Succession CSE 1000 Release 1.x systems that were added in an earlier version of OTM cannot be converted to a Succession CSE 1000 Release 2.0 system. You must delete the Release 1.x system and add a new Succession CSE 1000 Release 2.0 system.

You can add as many as 256 systems (including non-Succession CSE 1000 systems) to a site. You must have administrator privileges to add a system.

- 1 In the Navigator window, select the desired site.

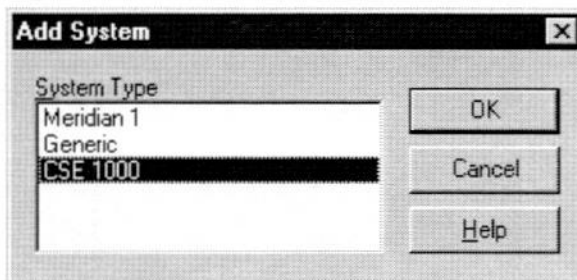


Note: If you are adding a new system from within the New Site Properties dialog box, skip to step 3 in this procedure.

- 2 Choose Configuration > Add System, or use the right mouse button pop-up menu.

The Add System dialog box appears (Figure 70).

Figure 70 Add System dialog box—Succession CSE 1000



- 3 In the Add System dialog box, select CSE 1000 and click OK.



Note: You may need to install additional software to enable other system types not listed in Figure 70. Follow the installation instructions included with your order.

The System Properties dialog box appears with the General tab selected (Figure 71).

Figure 71 System Properties dialog box—General tab

Sample Site - Sample CSE - System Properties

General | Communications | System Data | Applications | Customers | Network

System Name **Short Name** **System Type**
Sample CSE SCSE CSE 1000

System Location ☒ Same as Site
Address 2305 Mission College Blvd.
City Santa Clara State/Province CA
Country USA Zip/Postal Code 95052

Contact Information ☒ Same as Site
Name Administrator
Phone Number 555-1212 Job Title System Admin.
Comments

OK Cancel Apply Help

- 4 Enter the System Name, Short Name (required fields), and other information as needed. Click Apply.

You can make system location and contact information the same as site information by clicking the “Same as Site” check box.



Note: Bold fields indicate required information. To change a value, edit the field. Some fields may have a list of predefined choices. An arrow within a field indicates a drop-down list of choices. Press the arrow to select from the list. For more detailed information, refer to the online Help.

- 5 To add a new communications profile, click the System Properties dialog box—Communications tab.

This tab defines the types of communications profiles that may be applied to system applications (one profile may be used for multiple applications).

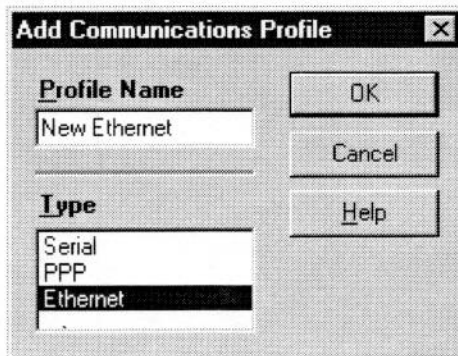


Note: OTM is shipped with a default communication profile. The Default profile is an Ethernet profile, and it cannot be deleted.

- 6 Click Add.

The Add Communications Profile dialog box appears (Figure 72).

Figure 72 Add Communications Profile dialog box

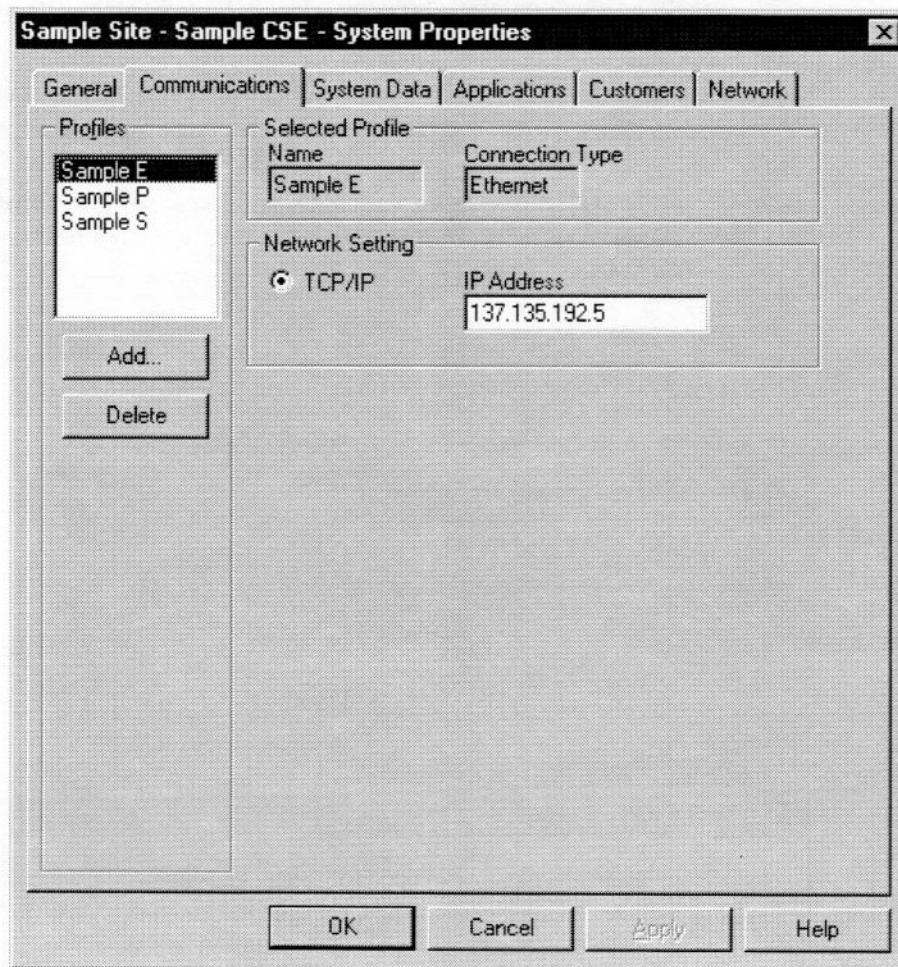


Select a communications type from the Type box and enter a Profile Name. Then click OK to return to the Communications tab.

7 Fill in the communications information for the new profile:

- For Ethernet (Figure 73):
 - Select the appropriate network protocol.
 - Enter the IP address that you configured on Succession CSE 1000 system.
 - Click Apply.

Figure 73 System Properties dialog box—Communications tab—Ethernet Profile



- For PPP (Figure 74):
 - Enter all modem parameters and dial-up information.
 - Select PPP in the Modem Script text box.
 - Set the IP address to the local IP address, as configured on the Succession CSE 1000 system.
 - Click Apply.

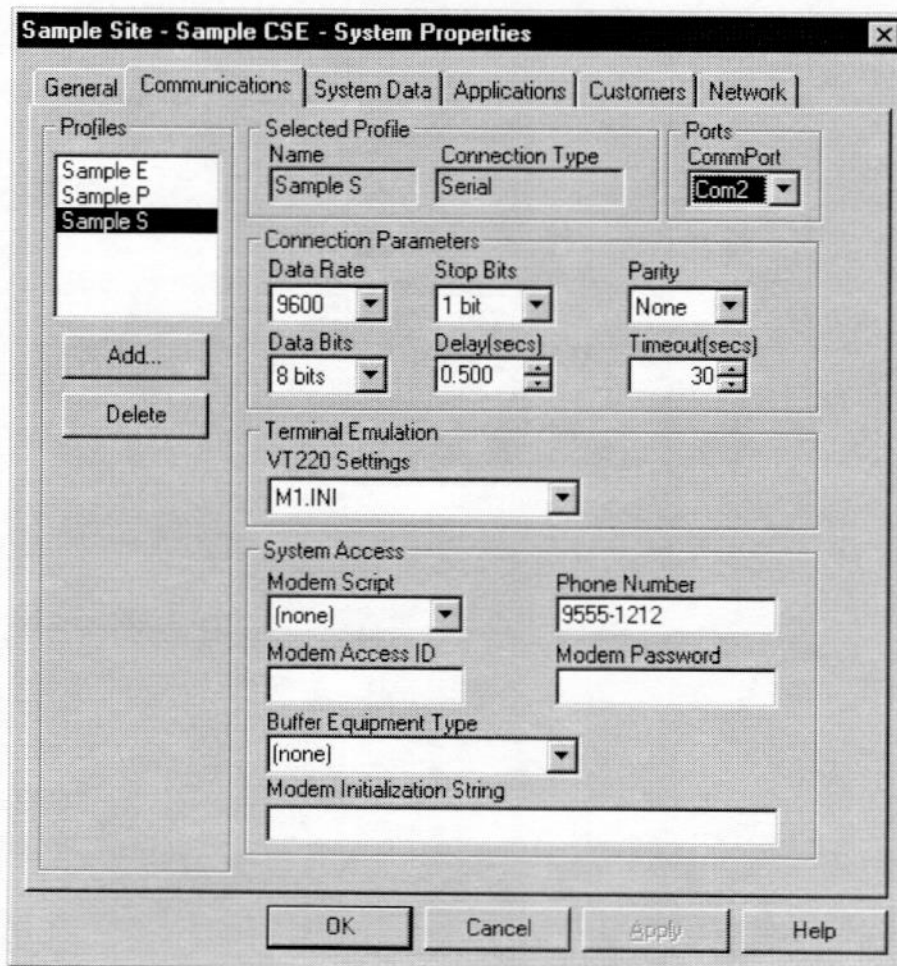
Figure 74 System Properties dialog box—Communications tab—PPP Profile

The screenshot shows the 'Sample Site - Sample CSE - System Properties' dialog box with the 'Communications' tab selected. The 'Profiles' list on the left contains 'Sample E', 'Sample P' (selected), and 'Sample S'. The 'Selected Profile' section shows 'Name' as 'Sample P' and 'Connection Type' as 'PPP'. The 'Port' dropdown is set to 'Com2'. The 'Connection Parameters' section includes 'Data Rate' (9600), 'Stop Bits' (1 bit), 'Parity' (None), 'Data Bits' (8 bits), 'Delay(secs)' (0.500), and 'Timeout(secs)' (30). The 'System Access' section has 'Modem Script' set to 'PPP', 'Phone Number' as '9555-1212', and empty fields for 'Modem Access ID', 'Modem Password', and 'Modem Initialization String'. The 'Network Setting' section has 'TCP/IP' selected and 'IP Address' as '137.135.192.6'. The bottom buttons are 'OK', 'Cancel', 'Apply', and 'Help'.

Sample Site - Sample CSE - System Properties			
General		Communications	System Data Applications Customers Network
Profiles Sample E Sample P Sample S Add... Delete		Selected Profile Name: Sample P Connection Type: PPP Port: Com2 Connection Parameters Data Rate: 9600 Stop Bits: 1 bit Parity: None Data Bits: 8 bits Delay(secs): 0.500 Timeout(secs): 30 System Access Modem Script: PPP Phone Number: 9555-1212 Modem Access ID: Modem Password: Modem Initialization String: Network Setting ☒ TCP/IP IP Address: 137.135.192.6	
OK Cancel Apply Help			

- For Serial (Figure 75):
 - Enter all modem parameters and dial-up information.
 - Select the appropriate value in the Modem Script drop-down box. This is usually None unless a specific value is defined for your system.
 - Click Apply.

Figure 75 System Properties dialog box—Communications tab—Serial Profile



8 Click the System Data tab.

The System Properties dialog box—System Data tab appears (Figure 76). Enter the machine/system type and release version for the system, and enable or disable feature packages. For example, if your system is a Succession CSE 1000 Release 2.0, use the drop-down boxes to select CSE 1000 in the Machine field and 2 in the Release field. When you have finished entering the information in the System Data tab, click Apply.

Figure 76 System Properties dialog box—System Data tab

Sample Site - Sample CSE - System Properties

General | Communications | **System Data** | Applications | Customers | Network

Machine Information

Machine: CSE1000 Release: 2

Issue: 0 System ID: Cutover Date: 1/18/2002

System Parameters

Maximum Speed Call Lists: 0 Maximum ACD Agents: 0

☐ MARP allowed ☐ Multiple Loop DN

PDI Password: xxxxxxxx

Packages

Enabled	Opt	Code	Description
	1	OPTF	Extended PBX Features
✓	2	CUST	Multi-Customer
✓	3	AIOD	Auto. Inden. of Out. Dial
✓	4	CDR	Call Detail Recording
✓	5	CTY	CDR - TTY
✓	6	CLNK	CDR - Mag. Tape
✓	7	RAN	Recorded Announceme
✓	8	TAD	Time and Date
✓	9	DNDI	Do Not Disturb-Indiv

Enable All Disable All

OK Cancel Apply Help



Note: You can copy this data directly from an installed switch by scheduling an upload using File > Update System Data in the System window. Update System Data uses the communication profile for Station Administration. However, you should configure the Release number here first to allow available applications to show up properly in the Applications Tab.



Note: In the System Parameters box, the PDT Password edit box allows you to set the Level 2 password for the Problem Determination Tool (PDT). If you change this password, you must manually change the PDT password on the system so that they match.

9 Click the Applications tab.

The System Properties dialog box—Applications tab appears (Figure 77).

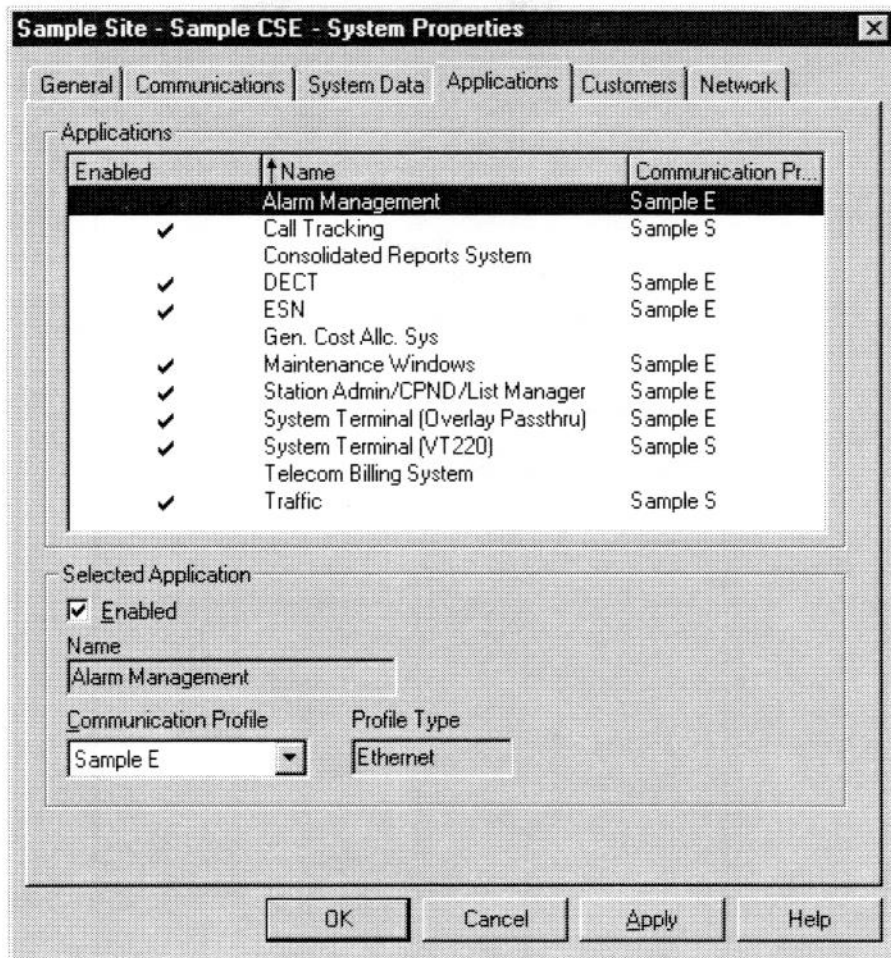
This tab defines the OTM applications that will appear in the System window and the communications profile to be used with each application.



Note: You must enable an application for it to be available in the System window.



Note: Communication profile settings are defined on a site/system basis and are shared by the OTM Server and its Clients. Consequently, if you define a serial communication profile for the Station Administration application, then both the OTM Server and OTM Client PCs must have a physical serial connection between the site/system and themselves. An OTM Client PC cannot use the COM ports of the OTM Server. Any communication task uses the resources of the PC on which it is running.

Figure 77 System Properties dialog box—Applications tab

To enable an application:

- a** Select the application in the Applications tab dialog box.
- b** Select a Communication Profile from the drop-down list in the Selected Application box.

A check mark appears next to the application, and the Enabled box is also checked.

To disable an application:

- a** Select the application in the Applications tab dialog box.

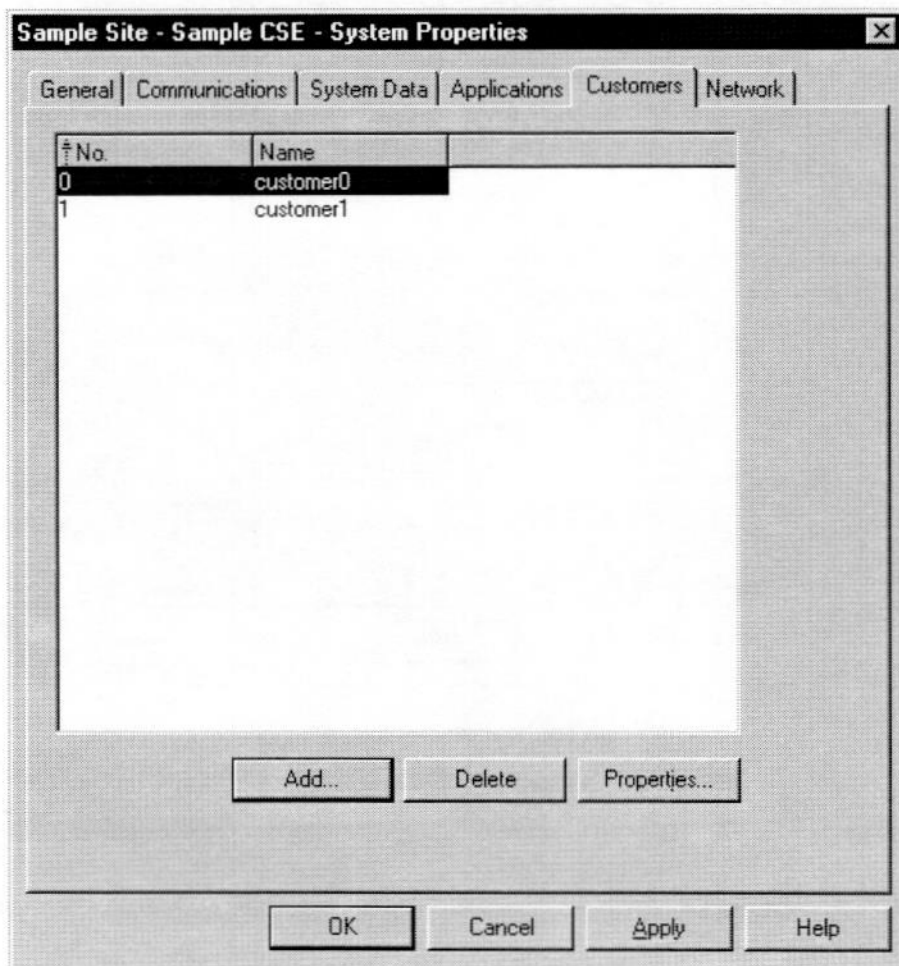
- b** In the Selected Application box, click the “Enabled” check box to remove the check mark.

When you have finished entering the information in the Applications tab, click Apply.

10 Click the Customers tab.

The System Properties dialog box—Customers tab appears (Figure 78).

Figure 78 System Properties dialog box—Customers tab



This tab lists the customers currently defined for this Succession CSE 1000 system. You may add new customers, delete customers, or review the properties of a selected customer. When you add a new customer, you configure the Succession CSE 1000 features and numbering plans that are available to the customer. This information is not automatically updated on the Succession CSE 1000 system and must be updated by using the LD 15 customer overlay. LD 15 is the overlay interface that allows customers to configure their systems on the Succession CSE 1000. For more information on overlay interfaces, see the System online Help.



Note: Customer information is required for System Administration/CPND and ESN applications.

11 To add a customer:

- a** Click Add in the System Properties dialog box—Customers tab.
- b** Select a Customer number.
- c** Click OK.

The Customer Properties dialog box—General tab appears (Figure 79).

Figure 79 Customer Properties dialog box—General tab

Customer1 - (Customer 1) Properties

General | Features | Numbering Plans

Customer Name **Number**

Directory Numbers

HLOC

Scheduler System ID

User ID
Password

OK Cancel Apply Help

- d** Fill in the general information for the customer.



Note: You can copy this data directly from an installed switch by scheduling an upload using File > Update System Data in the System window. Update System Data uses the communication profile for Station Administration. However, you should configure the Release number here first to allow available applications to show up properly in the Applications Tab.

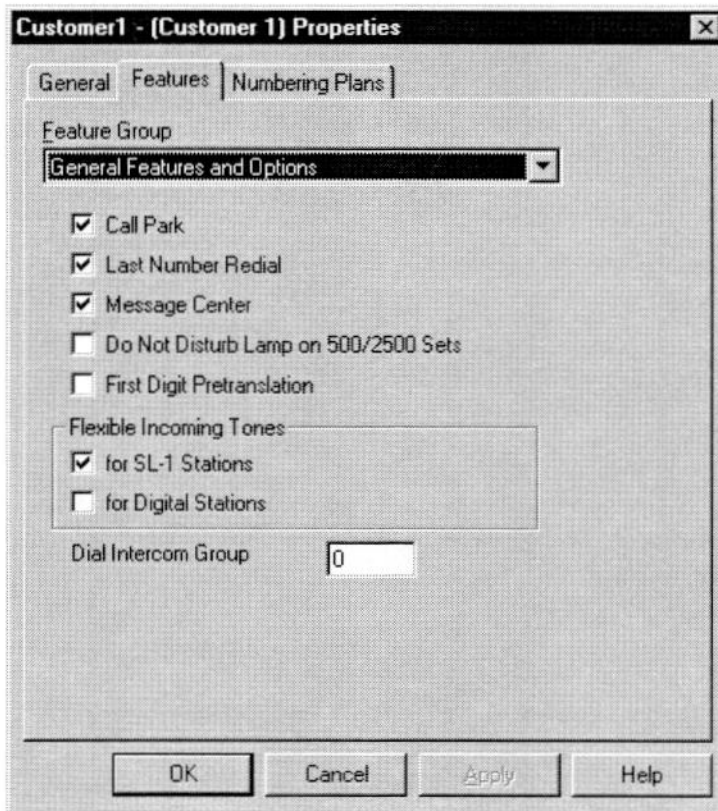


Note: Enter User information in the Scheduler System ID text box if you are using applications with scheduled activities, such as Station Administration/CPND, ESN, and Traffic Analysis.

- e** Click the Features tab.

The Customer Properties dialog box—Features tab appears (Figure 80).

Figure 80 Customer Properties dialog box—Features tab



- f** Fill in the feature information for the customer.
- g** Click the Numbering Plans tab.

The Customer Properties dialog box—Numbering Plans tab appears (Figure 81).

Figure 81 Customer Properties dialog box—Numbering Plans tab

Customer1 - (Customer 1) Properties

General | Features | **Numbering Plans**

DID	DN Type	from	to
	ACD DN	3000	3499
	ACD Position ID	3500	3999
✓	Regular DN	4000	4500

Selected Line

DN Type

Range: from **to**

☐ Direct Inward Dial Access Code Type:

Exchange

Usage

- h** Fill in the numbering plan information for the customer.
- 12** When you have finished entering the customer information, click one of the following buttons to save the information:
- OK adds the customer and returns you to the System properties sheet.
 - Cancel closes the dialog box without adding the customer.
 - Apply adds the customer and leaves the Customer properties open so that you can add other information for this customer.
- 13** To delete a customer, click Delete in the System Properties dialog box—Customers tab. A delete confirmation box appears. Click OK.
- 14** To modify customer information, click Properties in the System Properties dialog box—Customers tab. The Customer Properties dialog box appears with the General tab selected. Modify information in the appropriate tabs and click OK.

15 Click the Network tab.

The System Properties dialog box—Network tab appears (Figure 82).



Note: The Network tab is used to both add and delete Survivable Media Gateways and Branch Offices.

Figure 82 System Properties dialog box—Network tab

Sample Site - Sample CSE - System Properties

General | Communications | System Data | Applications | Customers | **Network**

Select the Gatekeeper Zone to which this switch belongs and define any Media Gateways.

Zone: **Sample Zone**

Primary Signaling Server: **47.21.111.5**

Alternate Signaling Server: **47.21.111.51**

Survivable Media Gateways and Branch Offices

Site	System	Type	Cabin
Sample Site	Sample Media...	Media Gatewa...	

- a Select the Gatekeeper Zone from the drop-down list, and enter the IP address or host name for the Primary Signaling Server. You may also define an Alternate (redundant) Signaling Server.

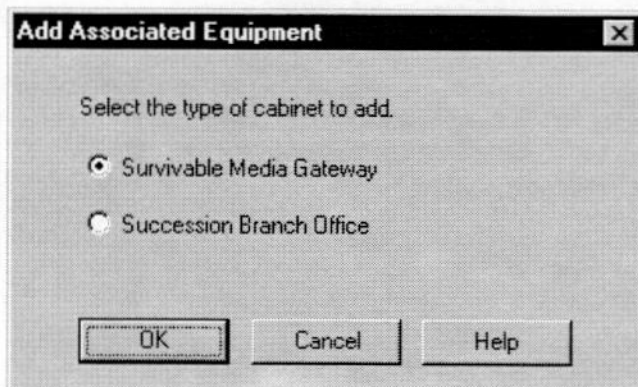


Note: For information on managing gatekeeper zones, see “Managing gatekeeper zones” on page 146.

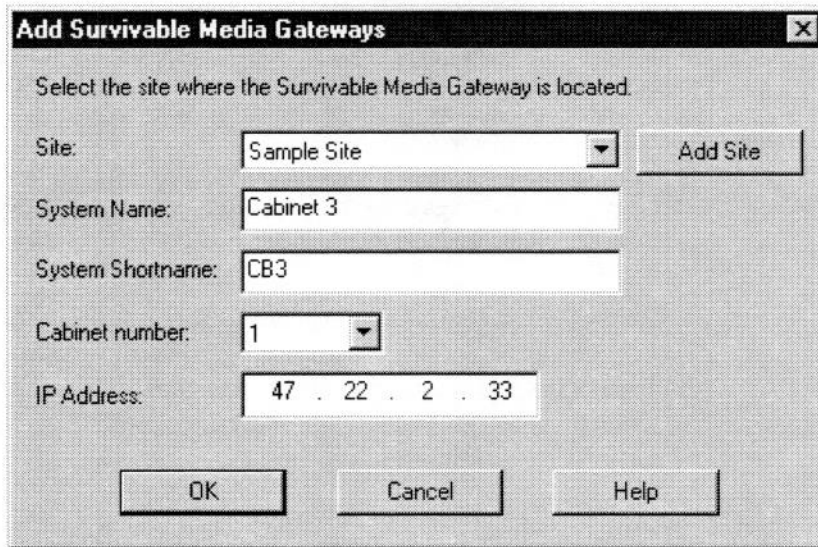
- b To add a Survivable Media Gateway or Succession Branch Office, click Add.

The Add Associated Equipment dialog box appears (Figure 83).

Figure 83 Add Associated Equipment dialog box



- c To add a Survivable Media Gateway:
Select Survivable Media Gateway and click OK.
The Add Survivable Media Gateways dialog box appears (Figure 84).

Figure 84 Add Survivable Media Gateways dialog box


The dialog box is titled "Add Survivable Media Gateways" and contains the following fields and buttons:

- Select the site where the Survivable Media Gateway is located.**
- Site:** A drop-down menu showing "Sample Site" and an "Add Site" button.
- System Name:** A text field containing "Cabinet 3".
- System Shortname:** A text field containing "CB3".
- Cabinet number:** A drop-down menu showing "1".
- IP Address:** A text field containing "47 . 22 . 2 . 33".
- Buttons:** "OK", "Cancel", and "Help".

Select the Site and Cabinet number from the drop-down lists, and enter the System Name, System Shortname, and IP address for this Media Gateway.

Click OK.

For additional information on the Succession CSE 1000 Media Gateway, see *Succession Communication Server for Enterprise 1000 Planning and Installation* (553-3023-210).

d To add a Succession Branch Office:

In the Add Associated Equipment dialog box (Figure 83 on page 142), select Succession Branch Office and click the OK button.

A new System Properties dialog box appears (Figure 85).



Note: A Branch Office contains a call processor for connection to the local PSTN and for analog devices such as FAX machines. IP telephones are located at the Branch Office; however, under normal conditions, call processing for these telephones is handled by the Call Server at the main office. The Branch Office and the Main Office are connected by IP Trunks, Virtual Trunks, or through trunks to the PSTN.



Note: IP telephones must be configured on both the Main Office and the Branch Office. Use Station Administration to add the telephones to both systems. You can copy and paste a telephone from one system to the other.

Enter the information in the System Properties dialog box—General, Communications, System Data, Applications, and Customers tabs as outlined in steps 4 through 14 of this procedure.



Note: Unlike a Media Gateway, a Branch Office has its own copy of call processing code, and may be running a different version of system software. For this reason, you must configure the System Data and Applications tabs as you would for a Call Server.



Note: A Branch Office must be associated with a Succession CSE 1000 Main Office, and both must be in the same Gatekeeper Zone.

For additional information on the Branch Office feature, see *Succession Communication Server for Enterprise 1000 Branch Office Guide* (553-3023-221).

Click the Network tab.

The System Properties dialog box—Network tab appears (Figure 85).

Figure 85 Branch Office System Properties dialog box—Network tab

Sample Site - Sample Branch Office - System Properties

General | Communications | System Data | Applications | Customers | Network

Define the location of the Main Office

Main Office: Sample Site-Sample CSE 1000 Properties

Primary Address: 47.11.20.10

Alternate Address: 47.11.20.11

Display in OTM Navigator:

As a Main Office
As a Main Office
As a Survivable Gateway

OK Cancel Apply Help

Select the Main Office from the drop-down list.



Note: You can click Properties to display the System Properties of the selected Main Office.

Click the Media Card radio button and enter the IP address or host name for the Media Card, or click the Signaling Server radio button and enter the IP address or host name for the Signaling Server. You may also define an Alternate (redundant) Signaling Server.

Use the drop-down list to select whether to display this Branch Office as a Main Office or as a Survivable Gateway in the OTM Windows and Web Navigators.

Click OK.

16 In the System Properties dialog box, click one of the following buttons:

- OK adds the system and closes the dialog box.
- Cancel closes the dialog box without adding the system.
- Apply adds the system and leaves the dialog box open.
- Help provides online Help.

The new system is added to the tree under the selected site.

Managing gatekeeper zones

Use the Gatekeeper Zones dialog box to add, delete, and change gatekeeper zones.

To add a gatekeeper zone:

- 1** In the System Properties dialog box—Network tab for a Meridian 1 system (Figure 67), or a Succession CSE 1000 Call Server (Figure 82), click Edit located next to the Gatekeeper Zone drop-down list.

The Gatekeeper Zones dialog box appears (Figure 86).

Figure 86 Gatekeeper Zones dialog box

Zone Name	Type	Primary Gatekeeper	Alternate Gatekeeper
Sample Zone	CSE 1000	47.11.30.1	47.11.30.2

Zone Name:

Primary Gatekeeper:

Address:

Mgmt URL:

Type:

Name:

Contact:

Location:

Alternate Gatekeeper:

Address:

Mgmt URL:

Type:

Name:

Contact:

Location:

OK Cancel Help

- 2 Enter a Zone Name. The Zone Name is required and must be unique. The Zone Name appears in the Windows and Web Navigators.
- 3 Enter the IP address of the Primary Gatekeeper.
- 4 Enter the management URL for the Primary Gatekeeper.
- 5 Use the drop-down list to select the type of gatekeeper:
 - CSE 1000 - for a Succession CSE 1000 call server
 - CS 3000 - for a Succession CS 3000
 - Other - for a third-party non-Nortel Networks gatekeeper
- 6 Enter a Name, Contact, and Location for the gatekeeper. These fields each have a maximum length of 30 characters. The Gatekeeper Name is required. The Contact and Location fields are optional.
- 7 If desired, you may assign an optional Alternate Gatekeeper to the zone by repeating steps 2 through 6 for the Alternate Gatekeeper.

- 8 Click Add to add the new gatekeeper zone to the list.
- 9 Click OK to close the Gatekeeper Zones dialog box and return to the System Properties dialog box—Network tab.

To modify the information on a gatekeeper zone:

- 1 In the System Properties dialog box—Network tab for a Meridian 1 system (Figure 67 on page 123) or a Succession CSE 1000 Call Server (Figure 82 on page 141), click Edit located next to the Gatekeeper Zone drop-down list.

The Gatekeeper Zones dialog box appears (Figure 86).

- 2 Select a gatekeeper zone from the list.
- 3 Edit the fields as desired.
- 4 Click Change.
- 5 Click OK to close the Gatekeeper Zones dialog box and return to the System Properties dialog box—Network tab.

To delete a gatekeeper zone:

- 1 In the System Properties dialog box—Network tab for a Meridian 1 system (Figure 67 on page 123) or a Succession CSE 1000 Call Server (Figure 82 on page 141), click Edit located next to the Gatekeeper Zone drop-down list.

The Gatekeeper Zones dialog box appears (Figure 86 on page 147).

- 2 Select a gatekeeper zone from the list.
- 3 Click Delete.
- 4 Click OK to close the Gatekeeper Zones dialog box and return to the System Properties dialog box—Network tab.

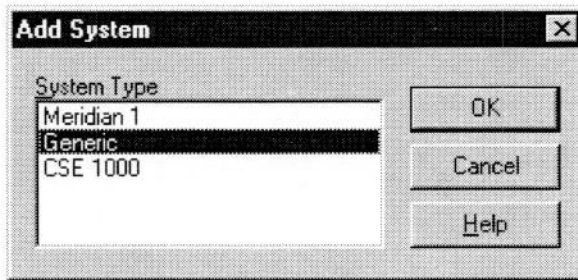
Adding a Generic system or device

You can add as many as 256 systems (including non-Meridian 1 systems) to a site. You must have administrator privileges to add a system.

- 1 In the Navigator window, select the desired site.
- 2 Choose Configuration > Add System, or right-click and select Add System.

The Add System dialog box appears (Figure 87).

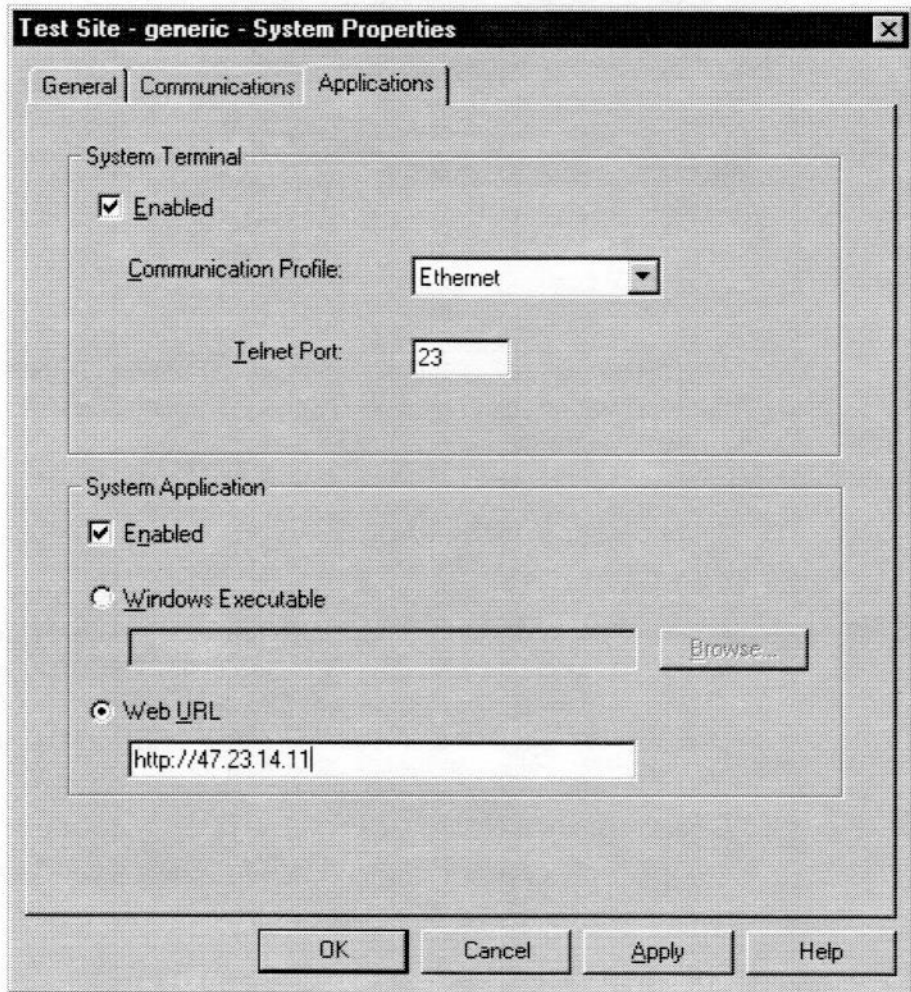
Figure 87 Add System dialog box—Generic



Note: You may need to install additional software to enable other system types not listed in Figure 87. Follow the installation instructions included with your order.

- 3 Select Generic in the System Type box.
- 4 Click OK.
- 5 Complete the System Properties dialog box—General and Communications tabs as you would for a Meridian 1 or Succession CSE 1000 system. See “Adding a Meridian 1 or Succession CSE 1000 Release 1.x system” on page 108, or “Adding a Release 2.0 Succession CSE 1000 system” on page 127.
- 6 Click the Application tab.

The System Properties dialog box—Applications tab for non-Meridian 1 devices appears (Figure 88).

Figure 88 System Properties dialog box—Applications tab for non-Meridian 1 devices

- 7 In the System Properties dialog box—Applications tab define the applications available for the device as follows:
- In the System Terminal section, select a Communication Profile. Typically, this is the Ethernet profile. Once defined, the user can double-click on the system in the Windows Navigator to launch the Windows System Terminal, or open a Web-based terminal window from the OTM Web Navigator Systems page, or both.

- In the System Application section, you have the option of launching a Windows executable or Web browser page for managing the device.

If a Windows executable is selected, it can only be accessed from the Windows Navigator. If a URL is selected, the Web site can be accessed from either the Windows or Web Navigators.

The availability of a terminal connection, executable, or Web site depends on the device.

Add OTM Windows users via the OTM Windows Navigator

OTM allows you to create User Groups to speed the process of adding users accessing the OTM Windows Navigator and certain OTM Web-based applications. In the User Group Properties dialog box, you define most aspects of certain kinds of users, such as their level of access to sites and systems and automatic connection to particular systems. You can create as many User Groups as you need. You assign individual users to a User Group when you add users to the OTM database.

There are two types of users: local users and remote users. Local users have accounts on the OTM Server. When you add a new local user, an OTM user account and a local Windows NT/Windows 2000 user account are created, and the account is assigned to the specified User Group. Deletion of a user removes the user account from the account list in Windows NT/Windows 2000, as well as from all relevant database tables. Remote users have accounts that exist on a domain controller or in an LDAP-compliant directory. For these users, OTM is used to assign the user ID for the account to an OTM user group.

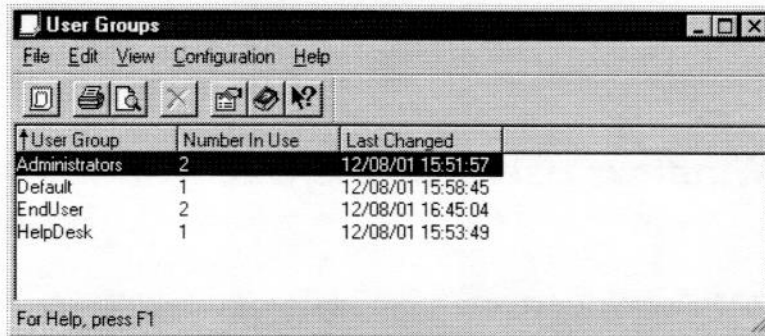


Note: Access to OTM Web Services is provided through the Windows NT/Windows 2000 server. A Windows NT domain account or an LDAP-compliant directory can also be used to authenticate OTM users for Web Services. Refer to “User authentication” on page 156.

Creating a user group

- 1 In the Navigator window, choose Security > User Groups to display the User Groups window (Figure 89).

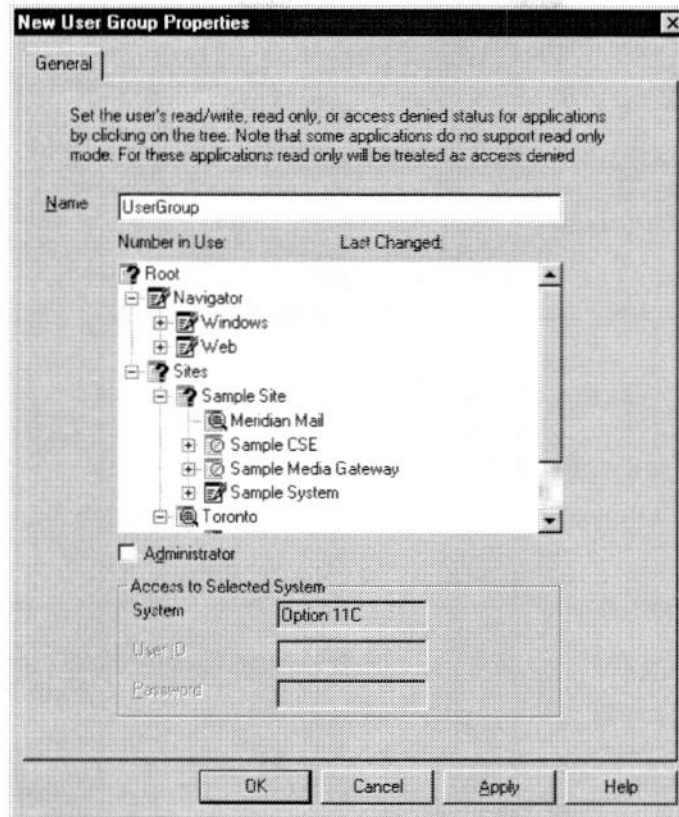
Figure 89 User Groups window



- 2 Choose Configuration > Add User Group. The new user group is created with the same access privileges as the highlighted user group. The New User Group Properties dialog box opens (Figure 90).



Note: The Administrators, Default, EndUser, and HelpDesk User Groups are always available and cannot be deleted. You can modify all groups except for Administrators. The Administrators User Group has access to all Windows-based and Web-based OTM applications.

Figure 90 New User Group Properties dialog box

3 Enter a name for this User Group.

For each site, system, and application in the tree, use the right mouse button to assign user privileges (Read-write, Read-only, or No Access). Each click of the right mouse button causes the access privileges and corresponding icon to change (Table 6). Select the Administrator box, if appropriate. The site and system icons change to reflect the access level.



Note: Access privileges defined for sites or systems at higher levels in the tree structure are applied to all subordinate items.



Note: The question mark icon indicates that the sub-items belonging to the item displaying the question mark icon have mixed access settings.

Table 6 Access privilege icons

Icon	Explanation
	Read and write access
	Read only access
	No access
	Indicates that the access privileges in the branch are mixed between one or more of the above levels

- 4 Enter values in the User ID and Password text boxes to allow this class of user to connect to this system without having to enter a User ID and Password each time you want to connect.
- 5 Click OK to save changes and close the User Group Properties dialog box.

Adding a user

- 1 In the OTM Users window, choose Configuration > Add User.
The User Properties dialog box opens (Figure 91).



Note: User accounts should be added here rather than through the Windows NT or Windows 2000 user management tools.



Note: The “Administrator” user account for the Windows NT or Windows 2000 OS does not appear in the OTM Users window. This is to prevent users from changing the Administrator account password from within OTM.



Note: Even though it is not listed in the Users window, the OS Administrator account can always be used to log in to OTM.

Figure 91 User Properties dialog box

2 Select a User Type from the drop-down list:

- Local - Users who are authenticated using an account on the OTM Server.
- Remote - Users who are authenticated using either a Windows NT Domain account or LDAP.



Note: When Remote is selected, the Change Password button as well as the Status and Current Status controls are disabled.

- 3** Enter a User ID.
- 4** From the User Group drop-down list, select the group that you will use as the basis for this user definition.
- 5** Fill in other data as required.
- 6** Click Apply. OTM prompts you to enter a password.
- 7** Click Change Password to change the OTM login password for this user only.

- 8 Click OK. The new user appears in the OTM User window. Close the OTM User window.

User authentication

You can select any of the following three methods or combination of these methods to authenticate OTM users:

- Local OTM Server account
- Windows NT Domain account
- LDAP authentication



Note: The Administrator account will always be authenticated through the local server account because it is a default account on all supported Windows platforms.



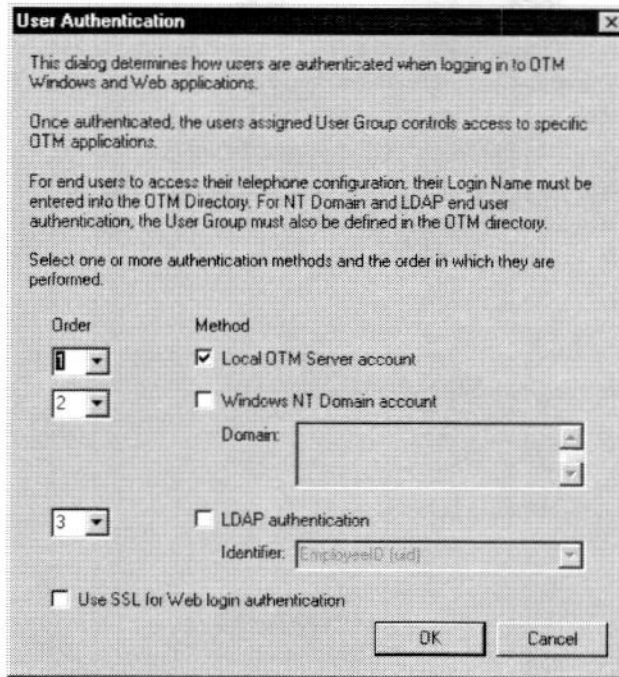
Note: The default authentication method is the Local OTM Server account. This method provides the best login performance because there is no requirement to search the OTM directory for the user's assigned User Group.

To configure authentication:

- 1 From the OTM Windows Navigator, select Security > User Authentication. The User Authentication dialog box appears (Figure 92).



Note: Authentication methods can also be configured using the Web navigator. See "User authentication" on page 162.

Figure 92 User Authentication dialog box

- 2 Use the check boxes to select one or more of the available authentication methods.
 - a If you select Windows NT Domain account, enter one or more domains in the Domain text box.
 - b If you select LDAP authentication, use the drop-down list to choose either EmployeeID (uid), or EMail (email).
- 3 Use the drop-down lists to assign the order in which the authentication methods are performed.



Note: If you choose multiple authentication methods, OTM respects the configured order; however, it should be noted that the best performance is achieved by using the Local OTM Server account method.

- 4 To use the secure socket layer (SSL) during the authentication process, click the “Use SSL for Web login authentication” check box.



Note: If the OTM Server has the required certificate installed, setting the check box and protecting specific virtual directories on the OTM Server causes OTM to SSL encrypted transport during authentication. In this case, Web login is performed using https:// rather than http://, and the traffic is encrypted. The OTM Server automatically switches to non-SSL transport once the user is successfully authenticated.

The selected method(s) are used to authenticate users on all OTM platforms: OTM Server, OTM Client, and OTM Web Client.

Adding OTM Web Navigator users

Access to the OTM Web Navigator is set up using the users and groups functionality in Windows NT and Windows 2000. User authentication can also be accomplished using Windows NT domain accounts or LDAP. Domain accounts and LDAP authentication are normally used for EndUsers who will be accessing Web Desktop Services to administer their telephones.

The OTM Web Navigator provides the following:

- A list of systems and devices; users click on a system or device to:
 - Open a Web System Terminal or URL to manage a system or device
 - Open Maintenance Pages for performing maintenance operations on M1 hardware
- Web-based alarm browser to view alarms and events from multiple systems and devices
- The ability to locate telephones, view, and change configuration data
- Web-based Maintenance Pages to perform maintenance operations (enable, disable, and so on) on Meridian 1 or Succession CSE 1000 system hardware
- OTM Web configuration pages (login access, LDAP sync reports, and so on)

The OTM administrator has the responsibility of installing, configuring, and maintaining OTM Web Services.

User login and security

Users log into the OTM Web Navigator using their Microsoft Windows NT or Windows 2000 userID and password. Login security for OTM Web Services ensures protection against unauthorized entry and enforces access permissions for logged on users.

There are three categories of users:

- Administrators — OTM administrators
- HelpDesk — OTM Help desk users
- EndUser — OTM end users

In addition, there is a Default user category. Default users are able to successfully log in to the Web Navigator, but they do not have an access profile defined in their Directory record.

OTM administrators and Help desk users have user accounts in a Windows domain. End users may have accounts either in a Windows domain or through an LDAP server. Administrators must be set up in a Windows Administrator group on the server itself, not on a remote computer.

OTM administrators and Help desk users can access and change their own telephones through either the Web Navigator or the Desktop Services end user pages. Access to the end user pages requires the appropriate OTM directory setup (user login and user group) for these administrators and Help desk users.

OTM Web application access permissions are controlled by the administrator on a per-Windows user group basis. For example, the administrator may limit the OTM user's access to only some of the OTM Web-based functionality. The OTM Web Navigator controls access to applications by shielding Web links to which the user does not have access. The directories and files comprising those applications are similarly protected.

You configure Windows NT or Windows 2000 user groups and individual users using the Windows user interface on the OTM server. You then determine the access permissions for each user group by using the OTM Web Navigator page. For information about setting user access, refer to “User Groups” on page 164.



Note: As a security precaution, with any upgrade or reinstallation of OTM software, access profiles for all user groups except Administrator are reset. By using the Web Access Security feature, any member of the Administrator user group can log in and set up access profiles for members of the Help Desk, End User, and Default user groups.

When an administrator or Help desk user first points a browser to the OTM Navigator Web site, a check is performed to see if the user has the required OTM Java plug-in. If the plug-in is not installed, the administrator or Help desk user is given the option of downloading and installing the plug-in. This operation is similar to the standard download operations in that the user must download the plug-in to the user's hard disk, and then it installs itself onto the computer.

While the plug-in check is being performed, the OTM splash screen appears. If the plug-in is installed, or after installation of the plug-in, the user is taken to the login page.

The default OTM URL is the end user login page. To navigate to the administrator login page, place `/admin` after the OTM IP address or host name.

Access permissions

When OTM starts for the first time, the Administrator profile is the only active profile. You must assign access permissions for the other Windows NT or Windows 2000 Groups that you have set up on the OTM Server.

Administrator Group access permissions

Persons belonging to the Administrators user group on the OTM Server can log in to the OTM Web site and get unrestricted access. The Administrators group has unrestricted access by default. You are not able to alter access permissions for the Administrators user group.

Users of the OTM Administration Site belong to a distinct user group and are assigned the security profile for that user group. For example, the Administrators user group has access to all Web applications.



Note: Important advice for localized operating systems — The name of the administrators user group in the French and German operating systems is not Administrators. These names are localized by Microsoft in the regional operating system software. In a default French installation of Windows NT or Windows 2000, the local administrators user group is Administrateurs. In the German version this user group is Administratoren. When installed on a French or German OS, the OTM predefined administrators user group will be named Administrateurs or Administratoren to match the OS.

User group access rights

You, the network administrator, log in to the OTM Administration Web site and assign access rights to the other user groups. By default, a member of any group other than Administrators does not have any access to OTM Web Applications unless you specifically grant that group appropriate permissions.

From the User Groups page, you grant or deny access to Web applications to a group, not to individual users. To change the security access for individual users, their group membership should be changed. For new groups, the Administrator must assign access rights for Web applications before any users from that group can log in. For information about setting user access, refer to “User Groups” on page 164.

With the exception of Administrators, do not place a person in multiple groups. The first group detected by OTM is used to determine access permissions. There is no restriction on the Administrators group. User may belong to other groups, but if they belong to the Administrators group, the Administrators profile overrides all other profiles.

While assigning access permissions, be certain that you select the top-level application for every sub-application that you assign. For example, if you are selecting System Alarms, you must also select Equipment. Failure to do so can result in members of the user group being denied access to the Web site.

User authentication

You can select any of the following three methods or combination of these methods to authenticate OTM users:

- Local OTM Server account
- Windows NT Domain account
- LDAP authentication



Note: The Administrator account is always authenticated through the local server account because it is a default account on all supported Windows platforms.



Note: The default authentication method is the Local OTM Server account. This method provides the best login performance because there is no requirement to search the OTM directory for the user's assigned User Group.

To configure authentication:

- 1 Under Web Administration in the OTM Web Navigator tree, select User Authentication.

The User Authentication page appears (Figure 93).

Figure 93 User Authentication page

Optivity Telephony Manager - Microsoft Internet Explorer provided by Nortel Networks

NORTEL NETWORKS Administrator Home Logout Help

OTM web navigator

- Equipment
- Web Station
- Telecom Billing Reports
- Web Administration
 - Custom Help
 - User Authentication
 - User Groups
 - Session Monitor

User Authentication

This page determines how users are authenticated when logging in to OTM Windows and Web applications.

Once authenticated, the user's assigned User Group controls access to specific OTM applications.

For end users to access their telephone configuration, their Login Name must be entered into the OTM Directory. For NT Domain and LDAP end user authentication, the User Group must also be defined in the OTM directory.

Select one or more authentication methods and the order in which they are performed.

Order	Method
1	☒ Local OTM Server account
2	☐ Window NT Domain account Domain:
3	☐ LDAP authentication Identifier: EmployeeID (uid)

☐ Use SSL for Web login authentication

Submit Reset

Click to expand Local intranet

- 2 Use the check boxes to select one or more of the available authentication methods.
 - a If you select Windows NT Domain account, enter one or more domains in the Domain text box.
 - b If you select LDAP authentication, use the drop-down list to choose either EmployeeID (uid), or EMail (email).

- 3 Use the drop-down lists to assign the order in which the authentication methods are performed.



Note: If you choose multiple authentication methods, OTM respects the configured order; however, it should be noted that the best performance is achieved by using the Local OTM Server account method.

- 4 To use the secure socket layer (SSL) during the authentication process, click the “Use SSL for Web login authentication” check box.



Note: If the OTM Server has the required certificate installed, setting the check box and protecting specific virtual directories on the OTM Server causes OTM to use SSL encrypted transport during authentication. In this case, Web login is performed using https:// rather than http://, and the traffic is encrypted. The OTM Server automatically switches to non-SSL transport once the user is successfully authenticated.

The selected method(s) are used to authenticate users on all OTM platforms: OTM Server, OTM Client, and OTM Web Client.

For information on configuring users for desktop access, see “Enable Web desktop access in the OTM Directory” on page 175.



Note: Authentication methods can also be configured using the Windows navigator. See “User authentication” on page 156.

User Groups

Navigator access is controlled by user group. A user’s User Group assignment determines which features are available on the Telephone features page. You also use the User Groups page to indicate which users are permitted to make changes to the General and Keys pages.

User groups must be added and deleted in the OTM Windows Navigator. See “Creating a user group” on page 152.

OTM is shipped with the following User Groups and corresponding access rights:

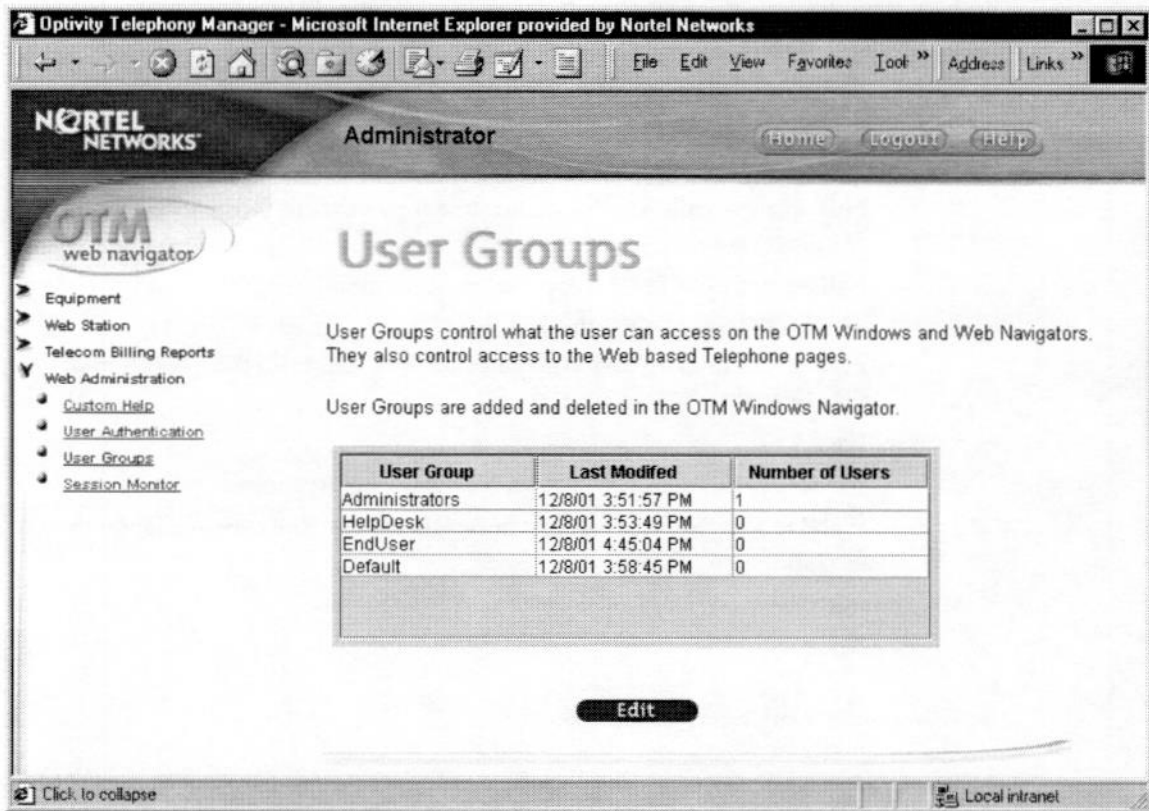
- Administrators
 - Full read/write access rights. Access rights cannot be changed for this user group.
- HelpDesk
 - Full access to all Web Navigator tree items except those under Web Administration.
 - Full access to Web Desktop Services, including read/write and synchronization capabilities.
 - Full access to Windows Navigator applications with the exception of ITG Services.
- EndUser
 - No access to Web or Windows Navigator applications.
 - Web Desktop Services is read only. Only 21 features are available; the rest are hidden.
- Default
 - No access.

To view the available User Groups:

- ➔ Click the User Groups link located under Web Administration in the OTM Web Navigator tree.

The User Groups page appears (Figure 94).

Figure 94 User Groups page



Navigator access

Access to the sites, systems, and applications available in both the Windows and Web Navigators is controlled on a user-group basis through the User Group Properties Java application.



Note: When the user group name is entered into the User Group field in an OTM user's Directory record, the entry must match the user group name exactly. This is primarily a concern when OTM is operating in a language other than English. In this case, the access profile name "HelpDesk" may have been translated into the local language.

To modify the access rights of a user group:

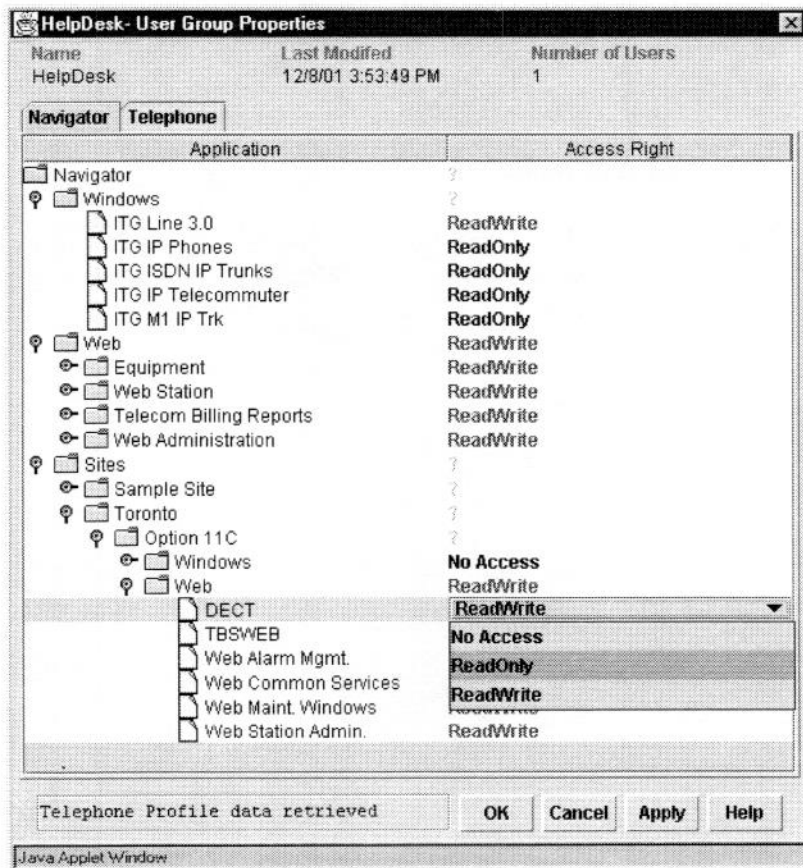
- 1 Click to select a User Group.
- 2 Click Edit.

The User Group Properties Java application launches, and the User Group Properties dialog box for the selected user group appears (Figure 95).



Note: Alternatively, you can double-click the user group to display the User Group Properties dialog box for the selected user group.

Figure 95 User Group Properties dialog box—Navigator tab



The Access Right column lists the level of access allowed for each site, system, and application. This is the same tree structure and performs the same function as the Windows-based New User Group Properties dialog box (Figure 90 on page 153).



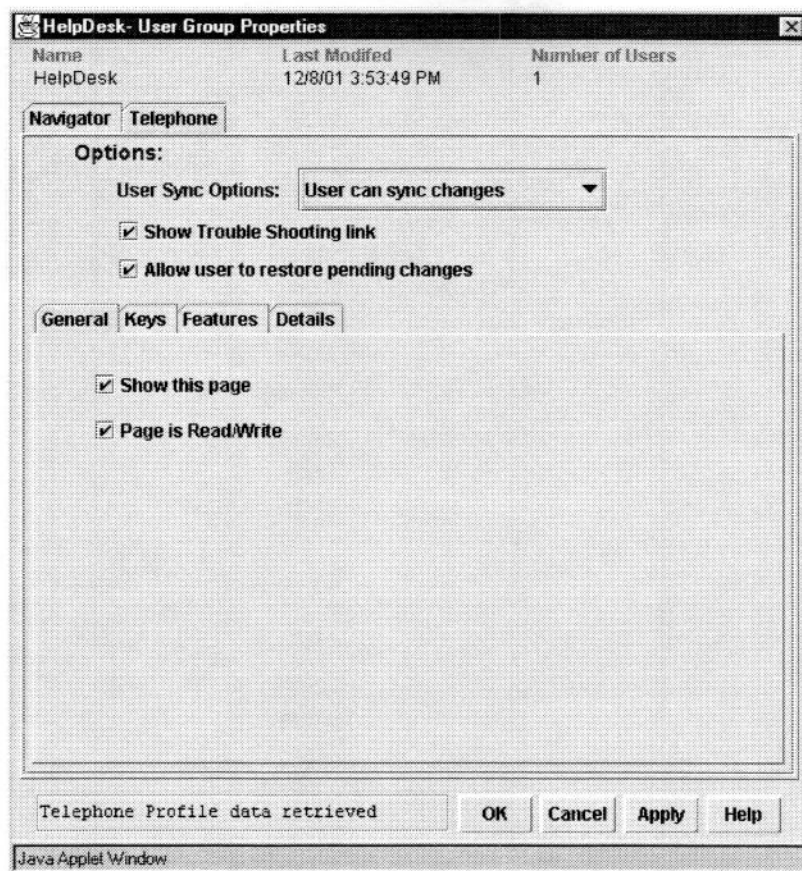
Note: The question mark indicates that the sub-items belonging to the item displaying the question mark have mixed access settings.

To modify access rights:

- 1 Use the drop-down list to select ReadWrite, ReadOnly, or No Access for each item in the tree.
- 2 Click Apply.

Telephone access

The Telephone tab in the User Group Properties dialog box is used to control access to the telephone pages on the Web for each user group (Figure 96).

Figure 96 Telephone access properties dialog box—General Tab

The options that are configured in the upper section of this dialog box are applicable to all of the tabs in telephone pages. These options include:

- Allowing or denying this group the ability to synchronize changes with the Meridian 1 or Succession CSE 1000 system. If synchronization is denied, you must manually synchronize the changes with the Meridian 1 or Succession CSE 1000 system using Station Administration.
- Determining whether the troubleshooting link appears at the top of the telephone page for members of this group
- Allowing or denying this group the ability to restore changes that have been made to a telephone

To configure telephone access options:

- 1 Use the drop-down list to select either “User can sync changes” or “User cannot sync changes.”
- 2 Click the “Show Trouble Shooting link” check box to enable this option.
For EndUsers, clicking the link displays the Telephone Troubleshooting Help page which includes a reset button.
For Web Navigator users, clicking the link displays the maintenance page for the telephone with all of the available commands.
- 3 Click the “Allow users to restore pending changes” check box to permit the users in this group to restore the changes made to a telephone.
- 4 Click Apply to apply your changes.

General tab

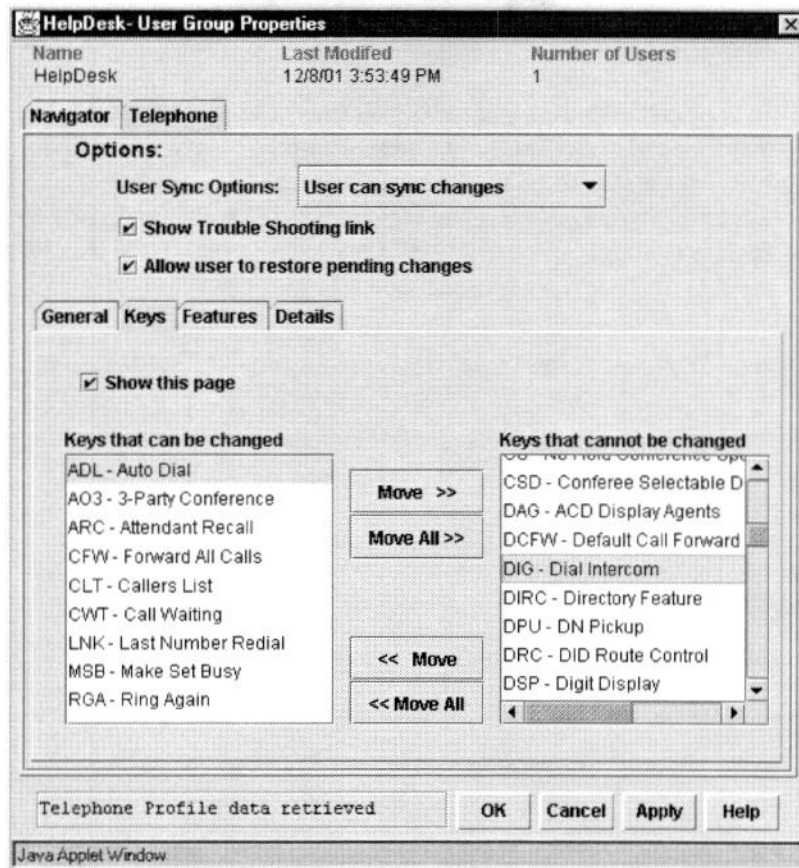
In the General tab, you use check boxes to determine whether the Telephone—General page will appear for this user group and whether the users in this group will be able to make changes to this Telephone page. The Telephone—General page contains information such as site, system, location, and TN, which may not be appropriate for or valuable to end users.

To configure the Telephone—General page:

- 1 Click the “Show this page” check box to allow this user group to be able to view the Telephone—General page.
- 2 Click the “Page is Read/Write” check box to allow users in this group to make changes to the information that appears in this telephone page.
- 3 Click Apply to apply your changes.

Keys tab

In the Keys tab (Figure 97), you use the check box and lists of key-based features to determine whether the Telephone—Keys page appears and, if so, which keys the users in this group can to change.

Figure 97 Telephone access properties dialog box—Keys tab

To configure the Telephone—Keys page:

- 1 Click the “Show this page” check box to allow this user group to be able to view the Telephone—Keys page.
- 2 Use the Move and Move All buttons to move the key-based features that this user group can change into the left column.

By putting keys into the left column, users in this group can interchange these key types and change the key parameters.



Note: If the user selects a key that is not in the left-hand column while viewing the Telephone—Keys page, the Change button does not appear.

- 3 Click Apply to apply your changes.

Features tab

In the Features tab (Figure 98), you use the check box and list of features to determine whether the Telephone—Features page appears and, if so, which features the users in this group can view and change. The list of features contains all the non-key features listed alphabetically by prompt in LD 10 and LD 11. Each feature is assigned a restriction of Hidden, ReadOnly, or ReadWrite. If Hidden, the feature does not appear in the end user Feature drop-down list.



Note: Read/Write capability requires the OTM Premium package.

Figure 98 Telephone access properties dialog box—Features tab

HelpDesk- User Group Properties

Name: HelpDesk Last Modified: 12/8/01 3:53:49 PM Number of Users: 1

Navigator | Telephone

Options:

User Sync Options: User can sync changes

☒ Show Trouble Shooting link

☒ Allow user to restore pending changes

General | Keys | Features | Details

☒ Show this page

Set each feature to be hidden, read only or read/write Show: ReadWrite

Mnemonic	Description	Restrictions
AAA	Automatic Answer Back	ReadWrite
AACD	Meridian Link Associated ACD Agent	Hidden
ABDA	CDR on Abandoned Calls	ReadOnly
ADAY	Alternate Redirection by Day	ReadWrite
ADCP	All-Digital Connection Prefix - Discon...	ReadWrite
ADV	Data Port Verification	ReadWrite
AEFD	Alternate External Flexible Call Forw...	ReadWrite
AEHT	Alternate External Hunt DN	ReadWrite

Telephone Profile data retrieved **OK** **Cancel** **Apply** **Help**

Java Applet Window

To configure the Telephone—Features page:

- 1 Click the “Show this page” check box to allow this user group to be able to view the Telephone—Features page.
- 2 Use the drop-down lists in the Restrictions column to configure each feature as ReadWrite, ReadOnly, or Hidden.



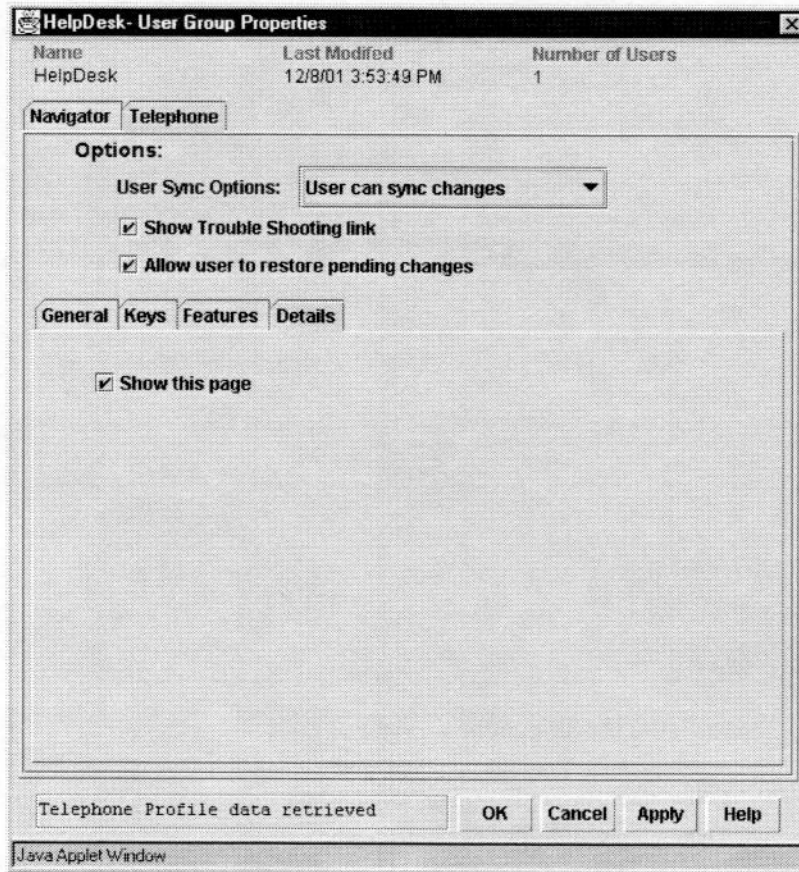
Note: The Show drop-down list contains All, Hidden, ReadOnly, and ReadWrite. This is used to limit the size of the list.

- 3 Click Apply to apply your changes.

Details tab

In the Details tab (Figure 99), you use the check box to determine whether the Telephone—Details page appears.

Figure 99 Telephone access properties dialog box—Details tab



Installing and Configuring Desktop Services

The following procedure outlines the steps that you must take to install and configure Desktop Services:

- 1 Install OTM. See "Initial installation tasks" on page 27.
- 2 Create Windows NT accounts for Help Desk users and End Users as required.

- 3 Log in to the Web Navigator as Administrator, and go to the Access Profiles page.



Note: To navigate to the Administrator Login page, place `/admin` after the OTM IP address or host name in your Web browser.

- 4 Configure the Help Desk, Default, and End User Access Profiles as desired.



Note: By default, Help Desk users are given read/write access to all features. Default and End Users have read-only access to 21 features.

- 5 Go to the Web Access Security page and set the Web Navigator access permissions for the Help Desk and Default user groups. See “User Groups” on page 164.



Note: To allow Help Desk users to make changes to other user’s telephone configuration data, make sure that they have access to the Find Telephones page.

- 6 Enter the Help Desk user’s Login Name and Access Profile in the user’s OTM Directory entry. See “Enable Web desktop access in the OTM Directory” on page 175.
- 7 Enter the End User’s Login Name and Access Profile in the user’s OTM Directory entry. See “Enable Web desktop access in the OTM Directory” next.
- 8 Select the desired Web Reporting Role in the user’s OTM Directory entry.

Enable Web desktop access in the OTM Directory

You can give End Users an account on the OTM server using the same process that is used to allow Administrators and Help Desk users to access the Windows and Web Navigators; however, End Users are typically authenticated through a Windows NT domain account or LDAP. End Users do not normally have accounts on the OTM Server. When the Windows NT domain or LDAP authentication method is used, mapping for the following attributes is performed using the OTM Directory:

- Login Name - required to associate users with their telephones

- User Group - determines what users can see and changes that they can make on their telephones
- Web Reporting Access Rights - controls access to Web TBS billing reports



Note: With LDAP, it is possible to determine the User Group during authentication. For this to occur, the LDAP directory must support the OTMUserGroup attribute, and return the User Group value with the authentication.

- 1 From Station Administration, select View > Employee Selector
- 2 Double-click an employee's name in the Employee Selector window.
The Employee Editor window for the selected employee appears.
- 3 Click the Additional Info tab in the Employee Editor window (Figure 100).

Figure 100 Entering Login Name attribute

Employee Editor

Employee | **Additional Info**

Attributes:

Type	Value	Publish
<New Attribute>		
Display Name	DALE COLDIRON	

* This attribute is read only.

Type: Login Name

Value: dale

Publish: ☐

Asset Association:

- Extension: 04
- Extension: 7007
- Extension: 7407
- Extension: 7429
- Extension: 7437
- Extension: 7544
- Station Location: 004-0-01-09*
- Station Location: 004-0-02-14*
- Station Location: 004-0-06-13*
- Terminal Number: 004 0 01 09*
- Terminal Number: 004 0 02 14*
- Terminal Number: 004 0 06 13*

OK Cancel Apply Apply/New Help

- 4 Select <New Attribute> in the Attributes pane.
- 5 Select Login Name from the Type drop-down box.
- 6 Enter the user's Windows NT Login Name for the attribute Value (if NT is the authentication method chosen for desktop users).
- 7 Click the "Publish" check box to enable synchronization with an optional LDAP-compliant server.
- 8 Click Apply in the Attributes pane.
- 9 Select <New Attribute> in the Attributes pane.
- 10 Select User Group from the Type drop-down box (Figure 101).

Figure 101 Entering User Group attribute

Employee Editor

Employee: Additional Info

Attributes:

Type	Value	Publish
<New Attribute>		
Display Name	DALE COLDIRON	
Login Name	dale	

* This attribute is read only.

Type: User Group

Value: EndUser

Publish: ☐

Apply Cancel Delete

Asset Association:

- Extension: 04
- Extension: 7007
- + Extension: 7407
- + Extension: 7429
- + Extension: 7437
- + Extension: 7544
- + Station Location: 004-0-01-09*
- + Station Location: 004-0-02-14*
- + Station Location: 004-0-06-13*
- + Terminal Number: 004 0 01 09*
- + Terminal Number: 004 0 02 14*
- + Terminal Number: 004 0 06 13*

OK Cancel Apply Apply/New Help

- 11 Enter EndUser for the attribute Value to enable End User Web desktop user access, both for LDAP and Windows NT access.

Enter HelpDesk for the attribute Value to enable Help Desk Web desktop user access, both for LDAP and Windows NT access.

- 12** Click Apply in the Attributes Pane.
- 13** Select <New Attribute> in the Attributes pane.
- 14** Select Web Reporting Access Rights from the Type drop-down box (Figure 102).
- 15** Enter one of the following access levels for the attribute value:
 - All - Users assigned this role have the authority to view all the reports for the site/systems to which they are assigned. This is the access level that you typically assign to an Administrator.
 - Peer - Users assigned this role have the authority to view the reports for all the entities in the same node in the Organizational Hierarchy and all its sub-nodes. This is the access level that you typically assign to a person who manages several departments.
 - Managed - Users assigned this role have the authority to view their own reports and the reports for all of the entities in the sub-nodes below their organization node in the Organizational Hierarchy. This is the access level that you typically assign to a department manager.
 - Personal - Users assigned this role have the authority to view their own data. This is the access level that you assign to a non-managerial employee.
 - No Access - If no role is assigned for a user, their reporting access rights default to No Access.

Figure 102 Entering Web Reporting Access Rights attribute

Employee Editor

Employee Additional Info

Attributes:

Type	Value	Publish
<New Attribute>		
Display Name	DALE COLDIRON	
Login Name	dale	
User Group	EndUser	

Asset Association:

- Extension: 04
- Extension: 7007
- Extension: 7407
- Extension: 7429
- Extension: 7437
- Extension: 7544
- Station Location: 004-0-01-09*
- Station Location: 004-0-02-14*
- Station Location: 004-0-06-13*
- Terminal Number: 004 0 01 09*
- Terminal Number: 004 0 02 14*
- Terminal Number: 004 0 06 13*

* This attribute is read only.

Type: Web Reporting Access Rig

Value: Personal

Publish: ☐

Apply Cancel Delete

OK Cancel Apply Apply/New Help



Note: For Desktop User Groups, you can use the Directory Update page in the OTM Web Navigator to simplify this process. See “Web Services” in *Using Optivity Telephony Manager* (553-3001-330).

If you have access to the Login Names in another database, consider using the Import/Export utility in the OTM System Window to simplify this process. See “Import and Export Utilities” in *Using Optivity Telephony Manager* (553-3001-330).



Note: “Appendix A” in *Using Optivity Telephony Manager* (553-3001-330) contains End User reference information. You can extract this appendix and distribute it as a user guide.

Setting Up the Meridian 1 or Succession CSE 1000 system

- 1 Verify that the Meridian 1 or Succession CSE 1000 system has the following system configuration:
 - The appropriate X11 release, configured with the appropriate packages
 - 48 MB or greater of memory on the Meridian 1
 - For Ethernet communications:
 - X11 Release 22 or later
 - IOP cards (Part number NT6D63BA or later), IOP/CMDU cards (Part number NT5D20BA or later) (not applicable to Option 11C systems), Release 22, or IODU/C cards (Part number NT5D61AB or later)
 - One or two Ethernet AUI cables (Part number NT7D90DA or later). You attach one cable to each IOP, IOP/CMDU, or IODU/C.
 - For Option 11C, an NTDK27AA Ethernet cable
- 2 For Ethernet networks, you need the following:
 - One or two Ethernet transceivers (different types for 10BaseT and 10Base2 cabling): attach one transceiver to each AUI cable
 - Ethernet communications cable: 10BaseT cabling requires Category 5 cable with RJ45 connectors



Note: Although normal phone cable and Category 5 cable are similar in appearance, phone cable is not acceptable for network applications.

- For 10Base2 cabling, an RG58 cable with BNC connectors



Note: Although normal television video coaxial cable and RG58 cable are similar in appearance, video coaxial cable is not acceptable for network applications.

- For the 10BaseT interface, an Ethernet hub



Caution: If you plan to connect the Meridian 1 or Succession CSE 1000 system to a corporate network, you require an Ethernet gateway or router to separate the system from the corporate network. If you connect the Meridian 1 or Succession CSE 1000 system without a gateway or router, you will adversely affect the system's call handling ability.

- 3 For PPP communication, you need the following:
 - Hayes command compatible modem
 - Modem cables
 - For Meridian 1 or Succession CSE 1000 SDI ports, user type MTC and SCH set in LD 17
- 4 For serial communication, you need the following:
 - Hayes command compatible modem only for remote dial-up
 - Modem cables
 - Direct serial cable connection between the PC and the SDI port on the switch
 - For Meridian 1 and Succession CSE 1000 SDI ports, the appropriate user type set in LD 17 for each OTM application (Table 7)

Table 7 SDI port settings for OTM applications

OTM application	SDI port setting
Station Administration	SCH
ESN	SCH
Telecom Billing System	CTY
Traffic Analysis	TRF if information is output to a buffer box; SCH if information is collected hourly from the Meridian 1 or Succession CSE 1000 system

- 5 Configure OTM users on the Meridian 1 or Succession CSE 1000 system:
User input is shown in **bold** following the > prompt (for example, >**LD 17**).

- Install the appropriate release (minimum is Release 22 for Meridian 1, and Release 25.30 for Succession CSE 1000) of X11 software.
- Perform an INIT.



Note: The OTM application will not function properly if an INIT has not been performed.

- Configure LAPW. OTM communicates with the Meridian 1 and Succession CSE 1000 systems through LAPW IDs and passwords configured on the Meridian 1 and Succession CSE 1000 systems.

>logi <ID>, where *ID* is the login ID.



Note: When a Limited Access Password (LAPW) is defined to collect traffic data from LD 2, configure the password to have access to all customers by setting the CUST prompt to **ALL**. For more information about Limited Access to Overlays, see *X11 Software Features Guide* (553-3001-306).

PASS?> <XXXXXX>, where XXXXXX is the level 1 or level 2 password.

WARNING: THE PROGRAMS AND DATA STORED ON THIS SYSTEM ARE LICENSED TO OR ARE THE PROPERTY OF NT/BNR AND ARE LAWFULLY AVAILABLE ONLY TO AUTHORIZED USERS FOR APPROVED PURPOSES. UNAUTHORIZED ACCESS TO ANY PROGRAM OR DATA ON SYSTEM IS NOT PERMITTED. THIS SYSTEM MAY BE MONITORED AT ANY TIME FOR OPERATIONAL REASONS. THEREFORE, IF YOU ARE NOT AN AUTHORIZED USER, DO NOT ATTEMPT TO LOGIN.

TTY #00 LOGGED IN 15:02 9/7/1996



Note: The following section is only required if login names are not configured.

>LD 17

```
CFN000
MEM AVAIL: (U/P): 3352174      USED: 203153      TOT:
3555327
DISK RECS AVAIL: 2764
DCH  AVAIL:      15      USED:      1      TOT:      16
AML  AVAIL:      10      USED:      0      TOT:      10
```

```
REQ> chg
TYPE> pwd
PWD2 (Your level 2 password)
LNAME_OPTION> yes
```

```
MEM AVAIL: (U/P): 3352174      USED: 203153      TOT:
3555327
DISK RECS AVAIL: 2764
DCH  AVAIL:      15      USED:      1      TOT:      16
AML  AVAIL:      10      USED:      0      TOT:      10
```

DEFAULT LOGIN NAMES SAVED



Note: At this point, your old passwords will work with either the newly assigned user IDs or with the default user ID values associated with your old passwords. See the online Help for LD 17, LNAME_OPTION for more information. Alert others of any changes (for example, all technicians with access to the Meridian 1 or Succession CSE 1000 system, the Distributor, and so on). Continue configuring LAPW and OTM.

```
REQ> chg
TYPE> pwd
PWD2 (Your level 2 password)
LNAME_OPTION> yes
NPW1
LOGIN_NAME
NPW2
```

LOGIN_NAME

LAPW> <n>, where n is the Limited Access Password

PWTP

PWn where n is the Limited Access Password

You will be prompted to enter your new password.

LOGIN_NAME> <xxxxxx>, where xxxxxx is your login name.

OVLA> all

OVLA

CUST> all

CUST

HOST

MAT> yes

MAT_READ_ONLY> no

OPT

LAPW

FLTH

LOCK

AUDT

INIT

MEM AVAIL: (U/P): 3352149 USED: 203178 TOT:
3555327

DISK RECS AVAIL: 2764

DCH	AVAIL:	15	USED:	1	TOT:	16
-----	--------	----	-------	---	------	----

AML	AVAIL:	10	USED:	0	TOT:	10
-----	--------	----	-------	---	------	----

REQ> end



Note: If you are using serial connections, skip this step. If you are using Ethernet or PPP connections, configure a PTY for each OTM application that will run simultaneously with other applications over Ethernet or PPP. For example, Maintenance Windows and System Terminal each require a PTY if they run at the same time. If you have enough free ports, Nortel Networks recommends that you configure at least two PTYs. You can allocate a maximum of 8 PTYs (maximum of 4 PTYs on an Option 11C or a Succession CSE 1000 system).

Find an empty TTY slot:

```
>LD 22
PT2000

REQ> prt
TYPE> adan tty

ADAN      TTY 0
CTYP PTY
DNUM 0
PORT 0
DES pty0
FLOW NO
USER SCH
XSM NO
TTYLOG      0
PORT 7
DES jonspty
FLOW NO
USER MTC SCH BUG
XSM NO
TTYLOG      0
BANR YES

ADAN      TTY 8
CTYP SDI2
DNUM 8
DES TECHSUN
FLOW NO
USER MTC SCH CTY BUG
XSM NO
TTYLOG      0
BANR YES

...

REQ> ****
OVL000
>LD 17
CFN000
MEM AVAIL: (U/P): 3352149    USED: 203178    TOT:
3555327
```

```
DISK RECS AVAIL: 2764
DCH  AVAIL:      15    USED:      1    TOT:      16
AML  AVAIL:      10    USED:      0    TOT:      10
```

Choose an empty port number between 0-15. Choose a PTY number 0-7. In this example, we find TTY 13 to be free, and assign PTY 0.

```
REQ> chg
TYPE> adan
ADAN> new tty <n>, where n is an available TTY port (0-15).
TTY-TYPE> pty
PORT> <z>, where z is an available PTY port (0-7).
DES> <n>
DES> new pty
FLOW
USER> mtc bug sch
TTYLOG
BANR
```

```
MEM AVAIL: (U/P): 3345946    USED: 209381    TOT:
3555327
DISK RECS AVAIL: 2764
DCH  AVAIL:      15    USED:      1    TOT:      16
AML  AVAIL:      10    USED:      0    TOT:      10
```

```
ADAN DATA SAVED
ADAN> end
```

6 Configure Ethernet and PPP at the Meridian 1 or Succession CSE 1000 system:



Note: The host names (*M1ACTIVEIP*, *M1INACTIVEIP*) and IP addresses used in the following instructions are only examples. Actual host names and IP addresses should conform to your network plan.

- In LD 117, configure an IP address at the Meridian 1 or Succession CSE 1000 system:

```
>LD 117
>NEW HOST M1ACTIVEIP 47.1.1.10
>CHG ELNK ACTIVE M1ACTIVEIP
```


- If you are using a backup (inactive) IOP, use LD 117 to configure it as well. This step does not apply to Option 11C Compact systems.
- The backup (inactive) IP is only used when the switch is in split mode.

```
>NEW HOST MINACTIVEIP 47.1.1.11
>CHG ELNK INACTIVE MINACTIVEIP
```

- Configure the subnet mask.
- If you have a default gateway in the network, define the routing table in LD 117.

```
>LD 117
>NEW ROUTE 47.1.0.0 47.1.1.250
```

The first four digits define the network IP address. The remaining digits specify the gateway IP address.

```
>PRT ROUTE (list the configured routing table)
>ENL ROUTE #, where # is the route number
```

If desired, you can print all information about route, host, gateway, and related settings.

The routing table provides the Meridian 1 or Succession CSE 1000 system with the IP address of the gateway server so the Meridian 1 or Succession CSE 1000 system can send return messages to the gateway for forwarding to the requesting client.

You can use **PRT ROUTE** for a list of routes with route numbers.

You can use **STAT ROUTE** to see if the route was successfully enabled.

- If you are using PPP, use the default addresses unless there is an address conflict. If a conflict exists, obtain a new IP address from your network administrator and configure this address.

```
>LD 117
>NEW HOST PPPLOCAL 47.0.0.2
>CHG PPP LOCAL PPPLOCAL MINACTIVEIP

>LD 117
>NEW HOST PPPREMOTE 47.0.0.3
>CHG PPP REMOTE PPPREMOTE MINACTIVEIP
```

- After you perform a series of **NEW**, **OUT**, **CHG** commands, type
 >UPDATE DBS
to clean up the database before you get out of LD 117.
- Use Overlay 137 to verify the IP address:
 >LD 137 (**Note:** Overlay 137 prompt is “. ”)
 .DIS ELNK (disables network)
 .ENL ELNK (enable Ethernet interface)
 .STAT ELNK (verify IP address)

If the **STAT ELNK** command displays the correct IP address, your IP address configuration is done. Otherwise, you must INIT the Meridian 1 or Succession CSE 1000 system.

Determining the OTM PC IP address

To find your PC's IP address:

- 1 From Start, select Settings > Control Panel. The Control Panel window appears.
- 2 Open the Network icon to display the tabbed dialog box. Click the Configuration tab. A list of installed network components is presented.
- 3 Select the TCP/IP network component used by your PC. Based on the number of installed components, you may have to scroll to see the correct component.
- 4 With the component selected, click Properties. The TCP/IP tabbed window appears.
- 5 Click the IP Address tab. Note the IP address shown. This is the IP address unique to this PC. You enter this information in Overlay 117 to specify where the alarm event will be received.
- 6 Close all the control panel-related windows and return to your desktop.

Enabling Meridian 1 and Succession CSE 1000 system alarms with LD 117

To enable alarms with LD 117:

- 1 In the OTM system window, on the toolbar, click the System Terminal icon.

The System Terminal Selection dialog box appears.

- 2 Click Ethernet/PPP (Overlay Passthru), and then click OK.

The System Terminal window appears.

- 3 Log in with the administrator user name and password.

You must have appropriate access privileges to use LD 117.

- 4 Enter:

```
LD 117
```

The => prompt appears in the Command Results pane indicating that the system terminal application is ready to accept your input.

- 5 Enter:

```
prt open_alarm
```

A list of slots currently in use appears. Slots are numbered from 0 through 7, for a total of eight available slots. Note the number of the next available slot.

- 6 Enter:

```
set open_alarm <n> <IP_address>
```

where *n* is the next available slot number and *IP_address* is the IP address of your OTM Server. See “Determining the OTM PC IP address” on page 188 for more information.



Caution: If you assign your IP address to a slot currently in use, it disconnects that user from the system preventing the user from receiving alarm information.

- 7 Enter

```
prt open_alarm
```

The list of slots and IP addresses receiving alarms appears. Verify that your particular slot and IP address are included.



Note: Overlay 117 accepts abbreviations of the various commands. For example, you can type the abbreviation `prt op` instead of `prt open_alarm`.

- 8 Log out and close the system terminal window.

Configuring Option 11C and Succession CSE 1000 systems for survivability

Configuring IP Line data for an Option 11C system

When distributing IP Line cards across different Survivable Expansion Cabinets, you can configure the Survivable Expansion Cabinets to each have their own node or to belong to the same node. If the Survivable Expansion Cabinets are not in the same location as the Main Cabinet, each Survivable Expansion Cabinet must have its own node.

This is related to which Survival IP address is configured on the IP Line cards. For a remote location, the Survival IP address of the IP Line cards on that node is the IP address of the SSC on that node. For situations where the Survivable Expansion Cabinets are in the same location as the Main Cabinet, the Survival IP address on all ITG line cards is configured to a single Survivable Expansion Cabinet SSC IP address.

The information below provides more information on these two options:

Survivable Expansion Cabinets in separate nodes for IP Line cards - Mandatory if Survivable Expansion Cabinets are in a different location than the Main Cabinet

- Trunks and Gateway channels are available in all Survivable Expansion Cabinets.
- More administration is required since there is more than one node to manage.
- If the IP Line card fails, IP telephones can register to another IP Line card only if it is contained within the same cabinet.
- Users cannot make IP telephone calls from one Survivable Expansion Cabinet to another.

Survivable Expansion Cabinets in the same node for IP Line cards

- Trunks and Gateway channels are only available for IP telephones on one Survivable Expansion Cabinet but can be used by all IP Line cards.
- Less administration is required since there is only one node to manage.

- If the IP Line cards fails, IP telephones can register to other IP Line cards in different Survivable Expansion Cabinets.
- Users can make IP telephone calls from one Survivable Expansion Cabinet to another.

Summary of steps to configure IP Line data on OTM

Refer to *Meridian 1 and Succession Communication Server for Enterprise 1000 IP Line; Description, Installation, and Operation* (553-3001-204) for a detailed description of these steps.

- 1 Manually add an IP Line card node. It is required that each Survivable Expansion Cabinet have its own node if the cabinets are not in the same location as the Main Cabinet.
- 2 Configure the IP Line card properties.
- 3 Configure the DSP profile data.
- 4 Configure the Main Cabinet ELAN IP address, Survivable Expansion Cabinet ELAN IP address, and TLAN voice port.

Enter the Meridian 1 ELAN IP address of the Main Cabinet.

Define the Survivable Expansion Cabinet IP address in OTM. There is an extra field in OTM to configure the Survivable Expansion Cabinet IP address and TLAN port. Use the same secondary IP address as the Survivable Expansion Cabinet's ELAN address. If the Expansion Cabinet is non-survivable, leave the default value of 0.0.0.0 (Figure 103).



Note: The ELAN IP address of the Survivable Expansion Cabinet must be on the same subnet as the Main Cabinet. If the Expansion Cabinet is on a different subnet, use the VLAN concept to keep both ELAN addresses on the same subnet.

- 5 Configure SNMP traps and the ELAN GW Routing table.
- 6 Configure security for SVMP access.
- 7 Configure the Alarm Notification feature in OTM.

Figure 103 ITG IP Phones - ITG Node Properties dialog box - Ports tab

ITG Node Properties - Sample Site - Sample System - Customer 0 - Node 1

General | Configuration | DSP Profile | SNMP Traps/Routing and IPs | **Ports** | Security

Enter the IP addresses and signaling ports. Changes must be transmitted to each ITG card

ELAN

Mendian1 IP: 10.123.124.110

Survival Cabinet IP: 0.0.0.0

Signaling port: 5000

Broadcast port: 5200

TLAN

Signaling port: 5000

Voice port: 5200

Restore Defaults

OK Cancel Apply Help

Configuring IP Line data for a Succession CSE 1000 system

When distributing IP Line cards across different Media Gateways, you can configure the Media Gateways to each have their own node or to belong to the same node. If the Media Gateways are not in the same location as the Call Server, each Media Gateway must have its own node.

This is related to which Survival IP address is configured on the IP Line cards. For a remote location, the Survival IP address of the IP Line cards on that node is the IP address of the SSC on that node. For situations where the Media Gateways are in the same location as the Call Server, the Survival IP address on all IP Line cards is configured to a single Media Gateway SSC IP address.

The information below provides more information on these two options:

Media Gateways in separate nodes for IP Line cards - Mandatory if Media Gateways are in a different location than the Call Server

- Trunks and Gateway channels are available in all Media Gateways.
- More administration is required since there is more than one node to manage.
- If the IP Line card fails, IP telephones can register to another IP Line card only if it is contained within the same cabinet.
- Users cannot make IP telephone calls from one Media Gateway to another.

Media Gateways in the same node for IP Line cards

- Trunks and Gateway channels are only available for IP telephones on one Media Gateway but can be used by all IP Line cards.
- Less administration is required since there is only one node to manage.
- If the IP Line cards fail, IP telephones can register to other IP Line cards in different Media Gateways.
- Users can make IP telephone calls from one Media Gateway to another.

Summary of steps to configure IP Line data on OTM

Refer to *Meridian 1 and Succession Communication Server for Enterprise 1000 IP Line; Description, Installation, and Operation* (553-3001-204) for a detailed description of these steps.

- 1 Manually add an IP Line card node. It is required that each Media Gateway have its own node if the cabinets are not in the same location as the Call Server.
- 2 Configure the IP Line card properties.
- 3 Configure the DSP profile data.
- 4 Configure the Call Server ELAN IP address, Survivable Media Gateway ELAN IP address, and TLAN voice port.

For the Meridian 1 ELAN IP address, enter the Succession CSE 1000 ELAN IP address of the Call Server.

Define the Survivable Media Gateway IP address in OTM. There is an extra field in OTM to configure the Survivable Media Gateway IP address and TLAN port. In the text box labeled Survivable Cabinet IP, enter the same secondary IP address as the Media Gateway's ELAN IP address. If the Media Gateway is non-survivable, leave the default value of 0.0.0.0 (Figure 103 on page 192).



Note: The ELAN address of the Survivable Media Gateway must be on the same subnet as the Call Server. If the Media Gateway is on a different subnet, use the VLAN concept to keep both ELAN addresses on the same subnet.

- 5 Configure SNMP traps and the ELAN GW Routing table.
- 6 Configure security for SVMP access.
- 7 Configure the Alarm Notification feature in OTM.

Transmitting IP Line node configuration data from OTM to the IP Line cards

Once the IP Line node and card properties are configured using the IP Line application within OTM, the data must be transmitted to the IP Line cards. OTM converts the configuration data to text files and transmits the files to the line cards.

Refer to *Meridian 1 and Succession Communication Server for Enterprise 1000 IP Line; Description, Installation, and Operation* (553-3001-204) for a detailed description of these steps.

- 1 Set the Leader 0 IP address using a TTY connected to the local RS-232 maintenance port.
- 2 Reboot Leader 0.
- 3 Transmit the node and card properties from the OTM ITG IP Phones application to Leader 0.
- 4 Reboot Leader 0.
- 5 Transmit the card properties to all of the cards in the node.

Setting up virtual terminal service

Virtual ports

In the Terminal Server application, the Virtual Ports Properties dialog box allows the OTM administrator to enable or disable a connection to a particular device. It displays the virtual port number for each configured device, and the corresponding serial or network settings. Launch the Terminal Server application by selecting Optivity Telephony Manager, and then selecting Terminal Server in the Windows Programs list in the Start menu.

To configure a virtual port:

- 1 Click Systems, or double-click the Configured Systems list.

If a device was selected in the Configured Systems list, then the corresponding device is also selected in the Virtual Port Properties dialog box. This allows the user to quickly change the settings for a particular device.

In the Virtual Port Properties dialog box, a tree displays the devices that can be connected via a virtual port. The tree lists the devices from the OTM database (configured using the OTM Navigator).

For a Meridian 1 or Succession CSE 1000 system, the VT220 profile is used (Ethernet/network or serial). If Ethernet/network is selected, the software uses the Meridian 1 or Succession CSE 1000 system's rlogin connection.

For a Generic system, the profile selected under the Application tab in System Properties dialog box is used (Ethernet/network or serial). If Ethernet/network is selected, the software uses a Telnet connection.

To enable virtual port connection for a device:

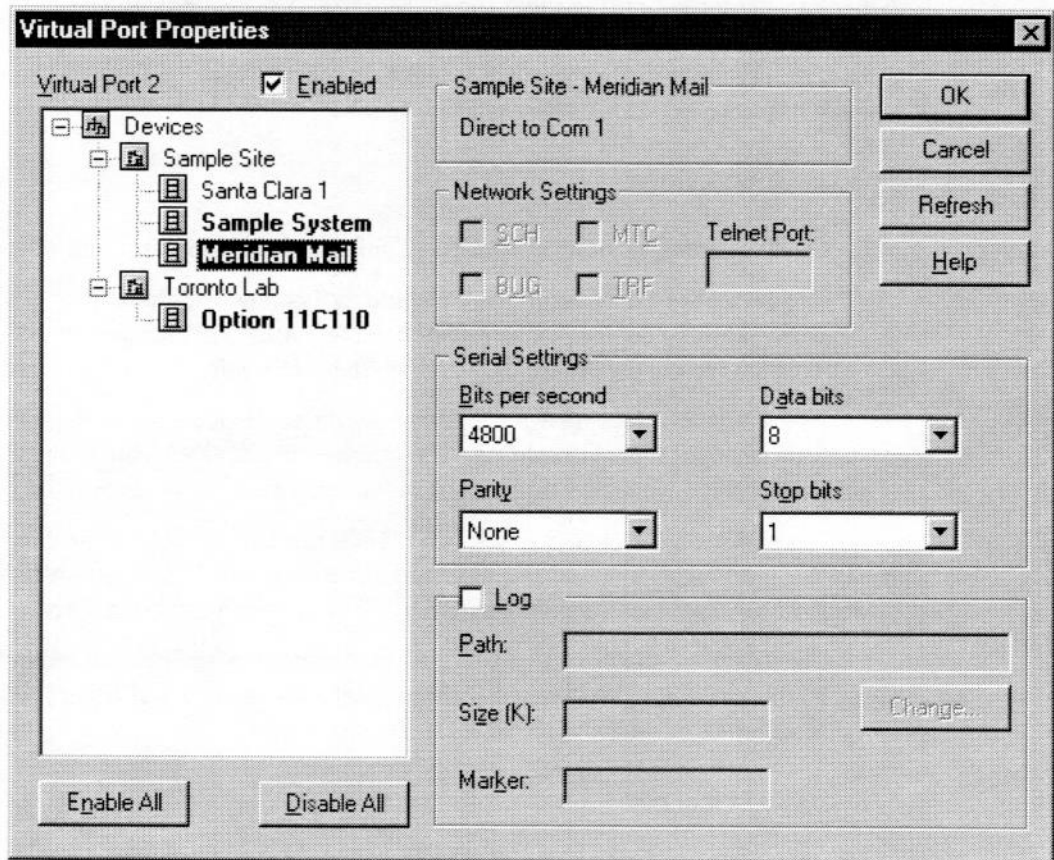
- 1 Do one of the following:
 - Double-click the disabled item in the tree.
 - Select the item, and check the Enabled check box.
 - Click Enable All to enable all the items listed in the tree with the default configuration.

The item becomes bold to show that it is enabled.

The field to the right of the Enabled check box automatically fills in the Site and System name for the device. This is the name that appears in the Terminal Server's main window.

For a serial connection, "Direct to Com *x*" appears, where *x* is the Com port number (Figure 104).

Figure 104 Configuring Virtual Ports (serial, logging disabled)



The fields for serial port settings are enabled. The default is the serial settings from the OTM database.

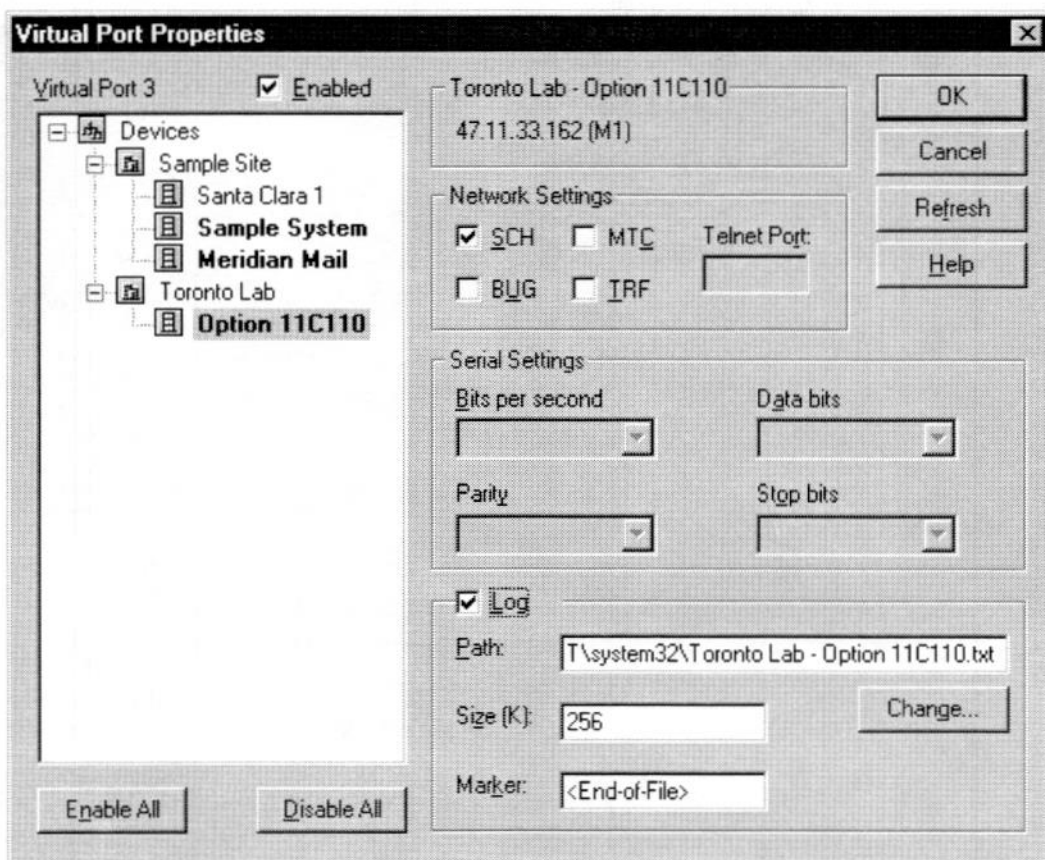
You can change the settings in the dialog box.

For a network connection, the IP address appears. It also displays whether the system is a Meridian 1 or Telnet.

- 2 Make sure the IP address is correct. If the IP address is different from the OTM database setting, click Refresh to update all network ports with the latest IP address from the OTM database.

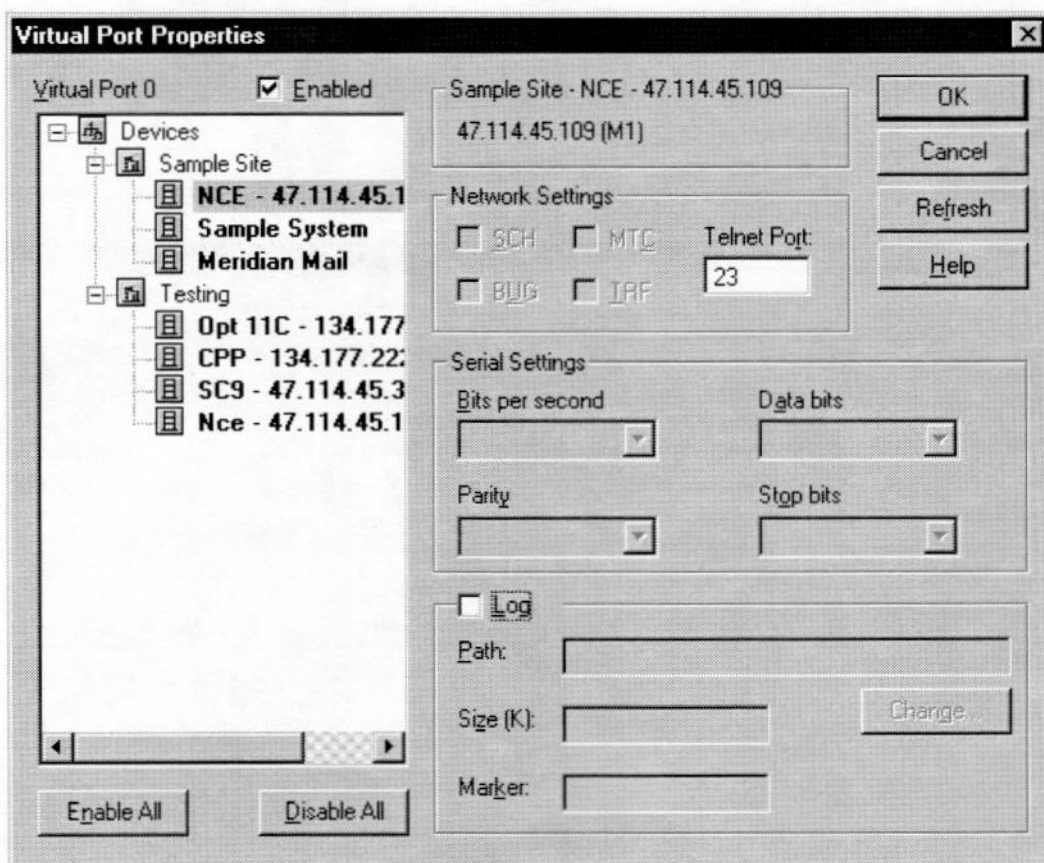
If you select a Meridian 1 or Succession CSE 1000 system, a Virtual Port Properties dialog box similar to Figure 105 appears.

Figure 105 Configuring Virtual Ports (Meridian 1 system, logging enabled)



- The fields for Meridian 1 port user types are enabled (default = SCH).

If you select a non-Meridian 1 system, a Virtual Port Properties dialog box similar to Figure 106 appears.

Figure 106 Configuring Virtual Ports (Telnet system, logging enabled)

- The fields for both serial and PTY user types are disabled. The border displays Telnet System and the selected device's IP address configured in OTM Navigator. In the Port field, you can specify a Telnet port number other than the port number specified in the Applications tab in the System Properties dialog box.

3 Check the “Log” check box to turn on data capture.

The log file name defaults to the Site and System name plus a .txt extension. You can change the path and the file name by typing in the edit box or clicking Change.

The maximum size of the log file is customizable (in the Size field) on a per-system basis, and defaults to 256 K. Once the file size reaches the limit, the Terminal Server starts from the beginning of the file, overwriting the oldest logs.

Due to the circular nature of the log, the Terminal Server writes an end-of-file marker, which is customizable in the Marker field, at the end of the log entries.

The log records the time and date when a client connects and disconnects to the virtual port, and writes all text received from and sent to the host. This allows a network administrator to keep an activity log of the virtual port connection.

If this ASCII log is to be viewed from a Web browser, the file should be stored in a Web-accessible path.

- 4 Click OK to store the changes, or click Cancel to discard them.
- 5 To disable a virtual port connection for a device, do one of the following:
 - Double-click an enabled item in the tree
 - Select the item and uncheck the Enabled check box
 - Click Disable All to disable all devices listed in the tree

The item is no longer bold, and does not appear in the Terminal Server main window when you click OK.

The Terminal Server application has a limit of 256 total configured ports/devices. It supports up to eight simultaneous serial connections.

However, the real limit on the number of simultaneous connections depends on the OTM server hardware, the network capacity, the server's CPU capacity, and so on.

Communication Settings

The Terminal Server uses TCP socket ports to communicate with the switch and Virtual Terminal Server. The Terminal Server, therefore, is not directly accessible through a network firewall, unless you enable the ports required. A network administrator determines the access method (for example, through dial-in accounts, enabling access to the ports used by Terminal Service, and so on).

The base port number determines the range of socket ports used to communicate with the Terminal Client. However, do not change this number unless the default port conflicts with another network application.

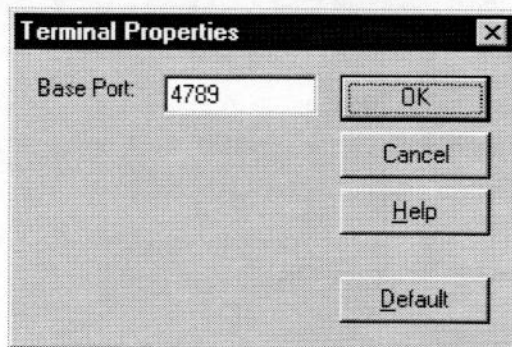
By default, the Terminal Server and Terminal Client communicate through network ports 4789 up to 5045 (4789 to send connection requests, 4790-5045 for up to 256 terminal sessions). Of course, the number of ports actually used depends on the number of virtual ports configured.

An administrator can change the range of port numbers by doing the following:

- 1 In the Terminal Server application, click Terminals.

The Terminal Properties dialog box appears (Figure 107).

Figure 107 Terminal Properties dialog box



- 2 Enter the new port number. Click Default to reset to the default value (port 4789).

For information on the Terminal Server Web Navigator Interface, see *Using Optivity Telephony Manager* (553-3001-330).

Setting up the Data Buffering and Access application

To configure a DBA Serial Port session:

- 1 From the Navigator window, choose Utilities > Data Buffering & Access.
The DBA main application window appears.

- 2 From the DBA Main application window, select File > New Session.
- 3 In the "Select an M1 System for Live session" dialog box, a tree displays the Site and Systems that can be used to collect serial data. Select a system from the tree to use for the new session.
- 4 In the New Session dialog box, select a Com port from the Connect Using combo box. The Connect Using combo box retrieves the available serial ports from the Registry. If you are using an Ethernet connection, then set Connect Using to Network.

Based on whether you have selected a serial or network connection, the fields that can be configured will be enabled.

- 5 Select Connect Now once you have configured the settings for the connection. If the connection is successful, the session window shows Connected in the window title. For serial connections, the session is connected if the port is available. This does not indicate that the device is connected to the serial port.

For more information on the Data Buffering and Access Application, see *Using Optivity Telephony Manager* (553-3001-330).

Setting up the LDAP Server

The LDAP Server utility allows you to link and synchronize the OTM and Corporate LDAP databases. OTM acts as an LDAP Client to the Corporate LDAP Server database.

You can use the LDAP Server to link an employee entry in the OTM directory to an entry in the LDAP directory. If employee data exists in the LDAP directory, you can select and add the employee entry into the OTM directory; or if the employee entry resides in both directories, you can select and link the entry.

When you link an entry between the OTM directory and the LDAP directory, OTM updates the entry's attribute data when you synchronize the directories. The following are examples of LDAP attributes:

- First name
- Last name
- Department

- Telephone extension



Note: Scheduled synchronizations only synchronize OTM Directory entries that have their Publish check box checked. Synchronization only compares and updates entries that have the same Unique Identifier (UID) in both the OTM Directory and the LDAP-compliant server. You can use the LDAP Synchronization Utility or the Import and Export Utility to manually set up the UID.

For detailed instructions on setting up the LDAP server, as well as an example of importing attributes to the OTM directory, see *LDAP Synchronization* in *Using Optivity Telephony Manager* (553-3001-330).

For information on importing non-LDAP-compliant directory information into the OTM directory, see *Import and Export Utilities* in *Using Optivity Telephony Manager* (553-3001-330).

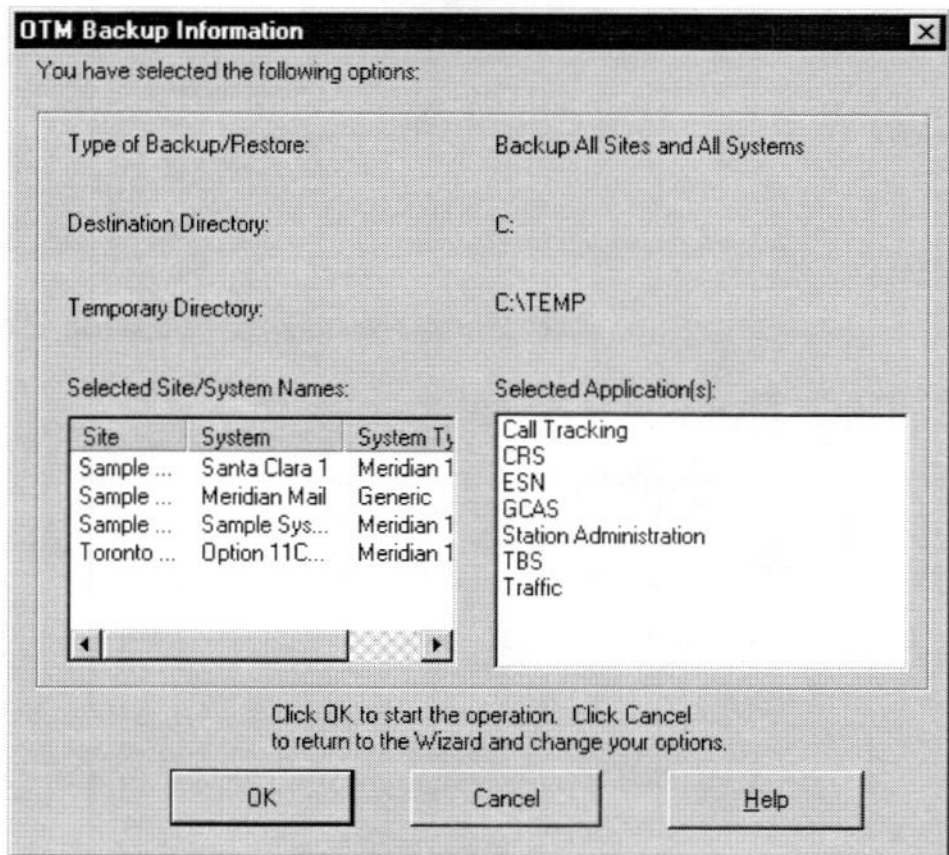
Setting Up Alarm Management

Configure each device to send traps to OTM, define the devices and scripts in Alarm Notification, and configure the DBA Serial and Rules Manager to receive serial text alarms and send SNMP traps. For more information, consult *Alarm Management* in *Using Optivity Telephony Manager* (553-3001-330).

Performing an OTM backup

To perform a backup of your OTM data and applications:

- 1 In the OTM Windows Navigator, select Utilities > Backup.
The OTM Backup Information dialog box appears (Figure 108).

Figure 108 OTM Backup Information dialog box

This dialog box summarizes the options selected for the backup:

- Type of backup (single site, single system, all sites and systems, or disaster recovery)
- Applications (Telecom Billing System, Call Tracking, ESN, Station, Traffic, GCAS, or CRS)
- Destination directory for backup files
- Temporary directory for working files created during the operation



Note: The destination and temporary directory screens display a computed space requirement for the files. You can back up and restore data for these OTM applications across multiple sites and systems at the same time.

- 2 Click OK to start the backup operation, or click Cancel to go to the backup wizard and change your options.

OTM Web browser Client installation

Make sure that the PC Client or UNIX workstation requirements have been met, as described in “OTM Windows Client requirements” on page 35.

Accessing the OTM Server Web Navigator via the PC Client

To access the OTM Server Web Navigator:

- 1 Enter the OTM Server IP address or computer name in the location bar of the Web browser on the PC Client.
- 2 Press Enter.

Software “plug-in”

The first time the OTM Server Web Navigator loads, you are prompted to download a software plug-in (Figure 109). The software you download is a standard Java Runtime Environment (JRE) “plug-in” of about 7-8 MB size.

Figure 109 JRE Plug-in download prompt



Integrating OTM with Optivity NMS

Optivity Telephony Manager (OTM) integrates with Optivity Network Management System (NMS) version 9.0.1 and above. Optivity NMS is an enterprise-level network management solution providing fault, performance, configuration, and security management for Nortel Networks inter-networking devices. Now through Optivity NMS, you can monitor your OTM Servers.

This section describes what you should know about integrating OTM with Optivity NMS. It includes the following information:

- “How the OTM with Optivity NMS integration works” next
- “Integration requirements” on page 207
- “The process of OTM–ONMS integration” on page 208
- “OTM OIT files” on page 209
- “Checklist for installing the Optivity Integration Toolkit” on page 209
- “About oitInstall” on page 210
- “Using Optivity NMS InfoCenter” on page 211
- “Viewing OTM Server Object Properties” on page 216
- “Modifying OTM Server Object Properties” on page 217
- “Starting OTM Web Applications” on page 217
- “Using FaultSummary” on page 219
- “Configuring OTM” on page 221
- “Removing an OTM Server” on page 222
- “Troubleshooting” on page 222

How the OTM with Optivity NMS integration works

OTM Alarm Manager receives Simple Network Management Protocol (SNMP) traps from managed Meridian 1 and Succession CSE 1000 entities. Through Alarm Notification, OTM sends filtered traps to Optivity NMS.

By using Optivity NMS InfoCenter, you can manually add OTM Servers into the Telephony Managers Resources folder. Property information that you add about the OTM Servers is added to the Optivity NMS database. For access to the Optivity NMS documentation, in your web browser go to <http://www.nortelnetworks.com/documentation>. Choose Optivity Network Management System in the Select a Product drop-down list, and click View Documents.

InfoCenter graphically identifies when a device is in an alarm state. By using Optivity InfoCenter, you can set the color for alarm levels. When a device is in an alarm state, you can right-click it to open an Optivity NMS fault management application. For instance, you can start Fault Summary that graphically lists faults for the selected device. You can also set the fault management categories for alarm monitoring.

Integration requirements

This section lists the conditions upon which OTM integrates with Optivity NMS optimally:

- For optimum performance, install OTM on a separate computer from Optivity NMS.
- For more information refer to the OIT support web site at <http://support.nortelnetworks.com>. See the procedure on page 208 for details.
- OTM integrates with Optivity NMS through OIT on any NMS platform. See “Checklist for installing the Optivity Integration Toolkit” on page 209. Coresidence with Optivity NMS, however, is supported only on Windows NT Server and Windows 2000 Server.
- All software requirements for OTM should be met. Particularly Windows NT Service Pack 6, Windows Option Pack 4, and MS Internet Information Server (IIS). Install IIS before applying the service pack.
- Always install Optivity NMS prior to installing OTM.



Note: There are certain restrictions in OTM application features when installed coresident with Optivity NMS. For more information about these restrictions, refer to the Optivity Telephony Manager (OTM) General Release Bulletin.

- Optivity NMS and OTM use different Web servers: Apache and IIS respectively.

In the OTM installation, when installing IIS, make sure that the default HTTP port 80 is not used by both the Apache and the IIS web servers.

- Change the Optivity NMS Apache Web server HTTP port from the default value of 80 prior to running IIS (Windows NT Option Pack 4) installation. If a port clash occurs, the default port on the Apache server must be changed.

The process of OTM–ONMS integration

The integration process in OTM 2.0 has been changed so that OTM does not automatically install any OIT files. You must manually install the OIT files. The OIT files can be downloaded from the OIT support web page. To download the OIT files:

- 1 In your web browser, go to <http://support.nortelnetworks.com>.
- 2 Click the View by a Product link.
- 3 In the drop-down list, select Optivity Network Management System OIT, and click Save,
- 4 In the drop-down list for software types, select Optivity NMS OIT for Optivity Telephony Manager.
- 5 Click the link under the Description heading that matches your operating system platform.
- 6 Click the link to the Readme file to view the installation instructions in your web browser. This file is also included in the zipped archive.
- 7 Click the link to the zipped archive to download the latest OTM OIT files.

Integration with ONMS versions prior to 10.0

When it detects ONMS, OTM no longer installs OIT files as part of the OTM installation process. You must manually install both the device and application OIT files to complete the integration process. The latest OIT files can be obtained from the OIT support web page.

Integration with ONMS version 10.0

ONMS version 10.0 comes pre-installed with the device OIT files required for releases of OTM prior to OTM 2.0. You must download and install the device OIT file for OTM 2.0 and the application OIT file manually. The application OIT file is common to all releases of OTM. These OIT files can be obtained from the OIT support web page. See the procedure on page 208 for details.

OTM OIT files

OTM 2.0 requires the following OIT files for integration with ONMS:

- NMS_otm_v10-B.oit
OTM Server device support entries
OTM Open Alarm II definitions
- NMS_otmApp_v10-B.oit
OTM Web Application integration entries

OTM also contains the following mib file:

- rfc1223.mib
Standard RFC 12313 MIB definitions

Run `oitInstall` for each .oit file, one at a time. The .mib file must be present in the same directory when `oitInstall` is executed. See step 5 under “Checklist for installing the Optivity Integration Toolkit.”

Checklist for installing the Optivity Integration Toolkit

This is the checklist for an OTM installation on an existing Optivity NMS server.



Note: This section provides general information on OIT. Refer to the NTPs, release notes, and read me files that are provided with your Optivity NMS software package for specific information on OIT.

You can install OIT files for OTM on any platform that runs Optivity NMS as long as it supports the Java Runtime Environment required by OTM Web Applications (JRE 1.3.1). In this case, the user should follow the steps in this section.

In the case of coresidence (only possible on Windows NT), the user only needs to understand the prerequisites and install OTM. OTM installation takes care of the OIT integration steps. Steps 1 through 6 as shown here are then not required.

1 Log into Optivity NMS as Administrator.

2 Check for the environment variable LNMSHOME.

In Windows NT, view environment variables using the System option in Control Panel on the Environment Variables tab. This variable holds the path of the Optivity installation (typically, c:\Optivity\NMS). All the executables are located in c:\Optivity\NMS\bin.

3 Check for the environment variable OITHOME.

This environment variable points to the Optivity Integration Toolkit home directory (typically, C:\Optivity\oit). If you cannot find OITHOME, create it.

4 Copy OTM OIT files to the appropriate subdirectories in OITHOME.

All of the subdirectories under \Optivity\Oit\ on the OTM CD-ROM are copied to OITHOME.

5 Run LNMSHOME\bin\oitinstall -u *<full path of OTM OIT file>* for every .oit file in the OTM directory, where -u indicates to upgrade Optivity NMS. If you do not specify the -u parameter, only a syntax check is performed on the OIT file.

This command updates the Optivity NMS database with the new definitions.

6 Proceed with OTM installation, checking for prerequisites (IIS, for instance) as always.

About oitInstall

Optivity NMS includes a program, oitInstall, that extracts the information that Optivity NMS needs for new device application support. This information includes:

- Database schema definitions
- MIB information

- Trap information
- Device management application launch points from within Optivity NMS applications
- Device discovery information



Note: For OTM, you must manually add the OTM Server.

OIT definitions for OTM reside in `$OITHOME\OTM\otm.oit`. It also contains the file `rfc1213.mib`.

The `$OITHOME` environment variable is typically `C:\Optivity\oit` on Windows NT systems, and `/usr/oit` on UNIX.

For platforms other than Windows NT, OIT definitions are updated into Optivity NMS by manually placing the OIT files into the appropriate directories and starting `oitInstall` from the command line.

The `oitInstall` program does the following:

- Automatically stops and restarts all Optivity NMS daemons (UNIX) or services (Windows)
- Automatically backs up the Optivity NMS databases, by default `/usr/oit/oitdb` for UNIX, and `C:\Optivity\oit\oitdb` for Windows. The `oitInstall` program automatically restores the database if the device support upgrade installation fails.
- Updates Optivity NMS with two new files: new device and device management support, and deletes the database backup if the integration is successful

Using Optivity NMS InfoCenter

Once OTM is integrated with Optivity NMS with the OIT definition files, you must manually add OTM server objects to the resources folders in InfoCenter. The OTM integration does not currently support Autodiscovery of these objects.

To configure Optivity NMS InfoCenter for OTM:



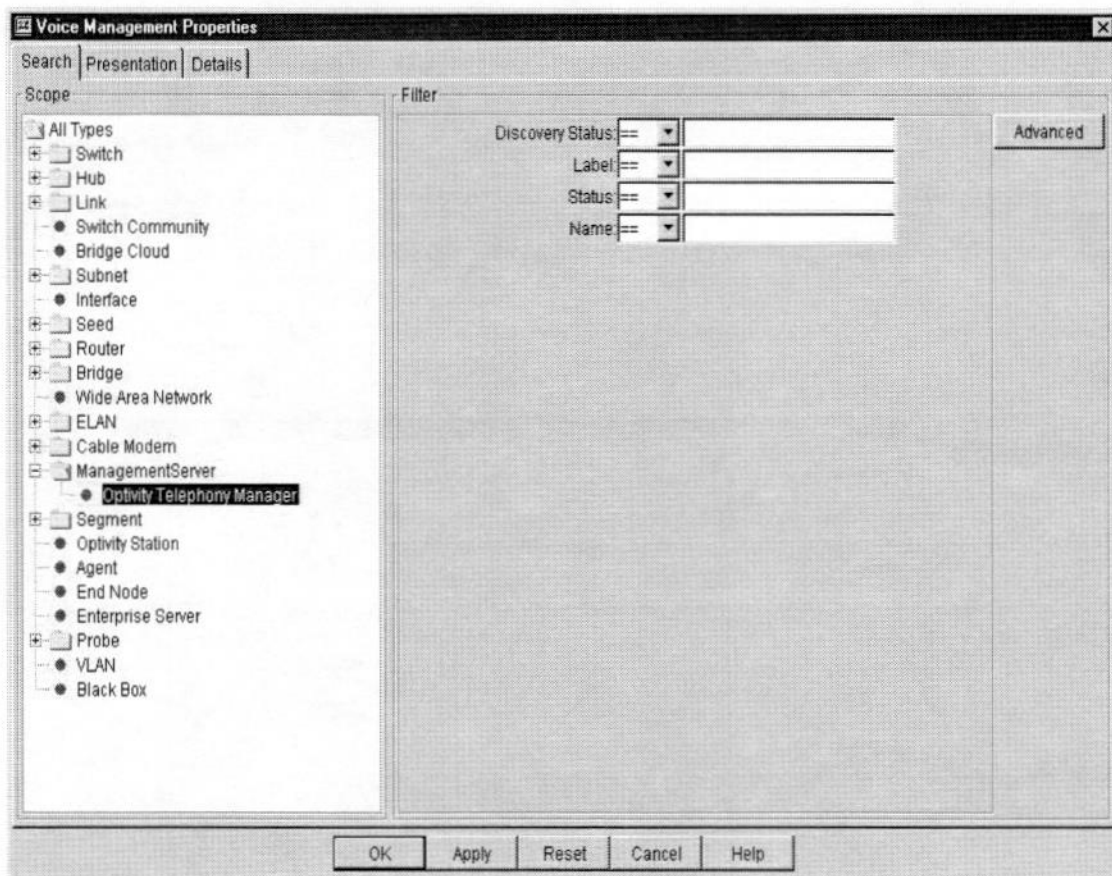
Note: You must be logged in as administrator / root to perform this activity.

- 1 Create a Voice Management folder in InfoCenter to contain all of the Voice Elements integrated into Optivity NMS (OTM in this case).
- 2 Modify the default Properties of the Voice Management folder to display the Optivity Telephony Manager objects added to this folder:
 - a Right-click the Voice Management folder and choose Properties (Figure 110).
 - b Open the ManagementServer folder.
 - c Select Optivity Telephony Manager (Figure 111 on page 214).
 - d Click Apply.

The Wizards provided in Optivity NMS 9.0.1 and above add new OTM servers to Optivity NMS. These wizards automatically take care of establishing the Device-Agent-Interface relationship in Optivity NMS databases.

Figure 110 InfoCenter Resources



Figure 111 InfoCenter Voice Management Properties dialog box

Adding OTM Server Object to Optivity NMS InfoCenter

Add an OTM server resource for every OTM server that you integrate and monitor with Optivity NMS.

If Access Control is enabled, you must have a valid local user account (user name and password) and an Optivity NMS user account to log in to InfoCenter.

- 1 From the Windows Start menu, choose Programs > Optivity > InfoCenter.
The Optivity NMS InfoCenter login window appears.
- 2 Type your user name, password, and the name of the Optivity NMS server, and then click OK.

Optivity NMS InfoCenter appears.

- 3** In the Folders pane, click the InfoCenter icon.
- 4** Double-click the Resources folder to open it.
- 5** A Telephony Managers folder appears.
A Telephony Managers folder is created in Optivity NMS InfoCenter to contain all the Voice Elements integrated into Optivity NMS.
- 6** Double-click the Telephony Managers folder to open it.
- 7** Modify the default view properties of the folder or you cannot view the OTM Servers that are added to this folder.

Right-click the Telephony Managers folder and choose Properties. Open the Management Server folder. Select Optivity Telephony Manager, and click Apply.

- 8** From the InfoCenter menu bar, choose File > New > Object.

The Object Properties dialog box appears with the Device tab selected (Figure 112).

- a** In the Label box, type a label for the new object.
- b** In the Type box, select the Management Servers object type.
- c** In the Subtype box, select an Optivity Telephony Manager subtype for the object.
- d** In the IP address box, type the IP address of the object.
- e** Click Private or Global.

Private lets the local user see the device. Global lets all users see the new object.

- f** Click OK.

A default switch icon appears for the OTM Server.

Figure 112 InfoCenter Object Properties dialog box

Object Properties

Device | Link | Object

Label: OTM Lab - 1

Type: ManagementServer

SubType: Optivity Telephony Manager

IP Address: 134.177.222.121

MAC Address:

Database: ☐ Private ☒ Global

OK Apply Reset Cancel Help

Viewing OTM Server Object Properties

Follow these steps to view the properties of an OTM Server in InfoCenter.

- 1 In InfoCenter, open a folder in the Folders pane.
- 2 Select the OTM Server that you added.
- 3 From the InfoCenter menu bar, choose File > Properties.

The Object Properties dialog box appears, displaying the properties for the selected network object.

- 4 Click OK.

Modifying OTM Server Object Properties

Follow these steps to modify the properties of an OTM Server in InfoCenter:

- 1 In InfoCenter, open a folder in the Folders pane.
- 2 Select the OTM Server that you added.
- 3 From the InfoCenter menu bar, choose File > Properties.

The Object Properties dialog box appears, displaying the properties for the selected network object.

- 4 Edit the object properties that you want.
- 5 Click OK.

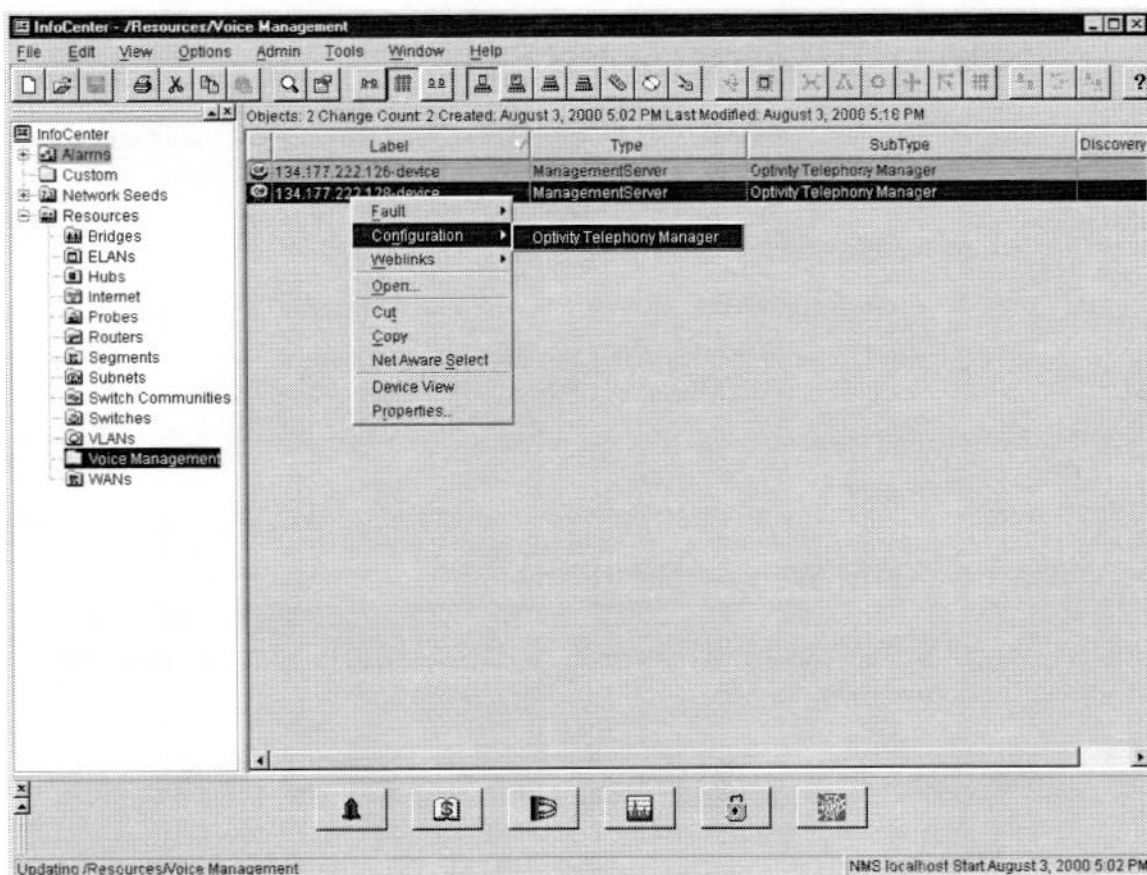
Starting OTM Web Applications

OTM Web Application links are integrated with Optivity NMS when an OTM Server is added.

The OTM system being accessed can be running on the same server as Optivity NMS (for Windows NT), or it can be connected remotely through the network.

You can start OTM Web Applications by choosing Configuration and selecting Optivity Telephony Manager from the shortcut menu on the OTM icon in Optivity NMS InfoCenter (Figure 113).

This action launches the default Web browser for your system and connects to the OTM Web Server. See “Java Runtime Environment for OTM and Optivity NMS” on page 218 for details on JRE.

Figure 113 Starting OTM Web Applications

Java Runtime Environment for OTM and Optivity NMS

OTM Web applications require Java Plug-In 1.3.1 on the client browser. Optivity NMS uses JDK 1.1.x, which is older than the version used by OTM.

JRE clash for OTM and Optivity NMS web clients

In both coresident and non-coresident situations, OTM and Optivity NMS applications cannot be launched simultaneously. The successful launch of OTM and Optivity NMS web applications accessing JRE depends on the version of JRE currently loaded in the system.

If a version of JRE that is different than 1.3.1 is loaded in the system and you access OTM web applications, you are prompted to install and load Java Plug-In 1.3.1 the first time that you try to connect to the OTM Server. With the Java Plug-In 1.3.1 loaded, OTM web applications load successfully.

If a version of JRE that is higher than 1.2.2 is loaded on the system, then Optivity NMS web applications that require JRE cannot be launched. This may occur even when the lower version is installed, but not loaded, on the system. To successfully launch Optivity NMS web applications, you must remove the higher version of JRE, and run the JRE 1.2.2 set-up program.

Web server

Optivity NMS uses Apache Web Server for its Web applications, whereas OTM uses Internet Information Server (IIS) from Windows NT Option Pack 4.

Using FaultSummary

OTM filters and then forwards Meridian 1 and Succession CSE 1000 traps to Optivity NMS. Since OTM forms the main representative agent for Meridian 1 and Succession CSE 1000 systems, all alarms received by Optivity NMS result in the change of status state of OTM depicted in Optivity InfoCenter.

When Optivity NMS and OTM coreside on the same server, the OTM Trap system disables its Trap Server and instead interfaces with the Optivity Trap Server to receive traps.

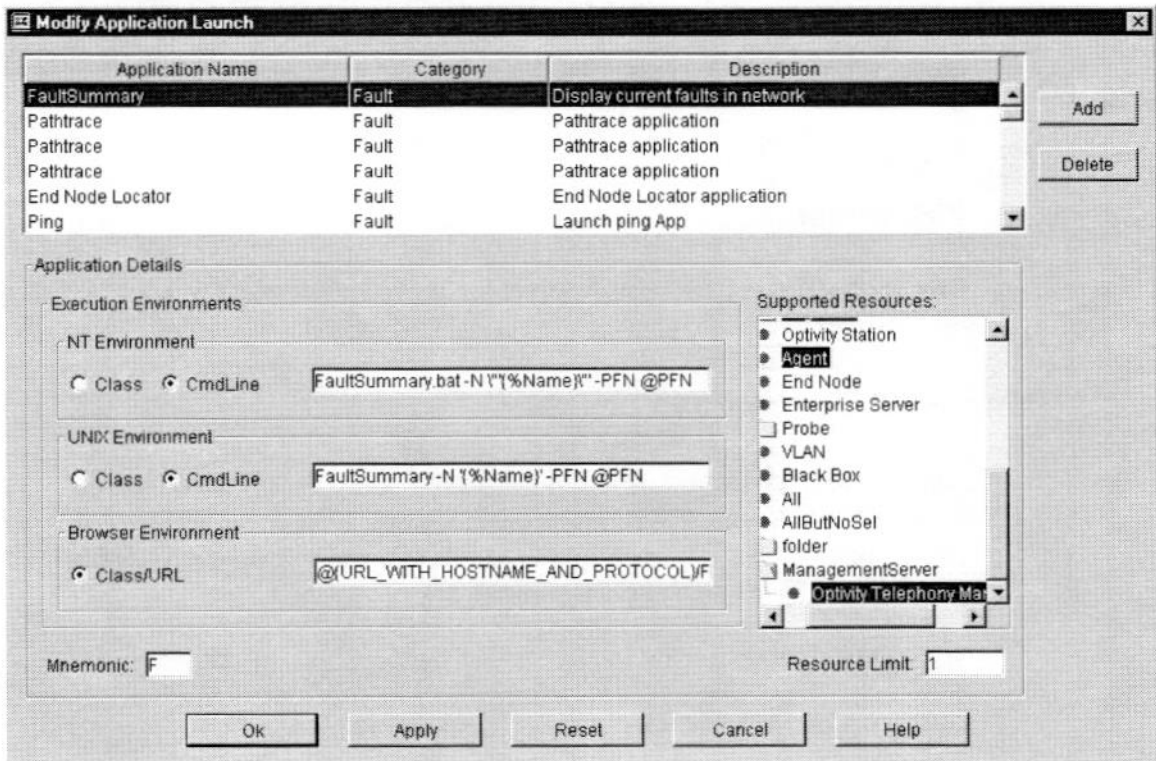
Upon receiving a Meridian 1 or Succession CSE 1000 alarm (or other traps that it has been configured to handle), OTM reformats it and forwards it to Optivity NMS. Optivity NMS recognizes the trap (from OIT definitions) and should now be able to reflect the changed status.

Setting up FaultSummary

To set up FaultSummary:

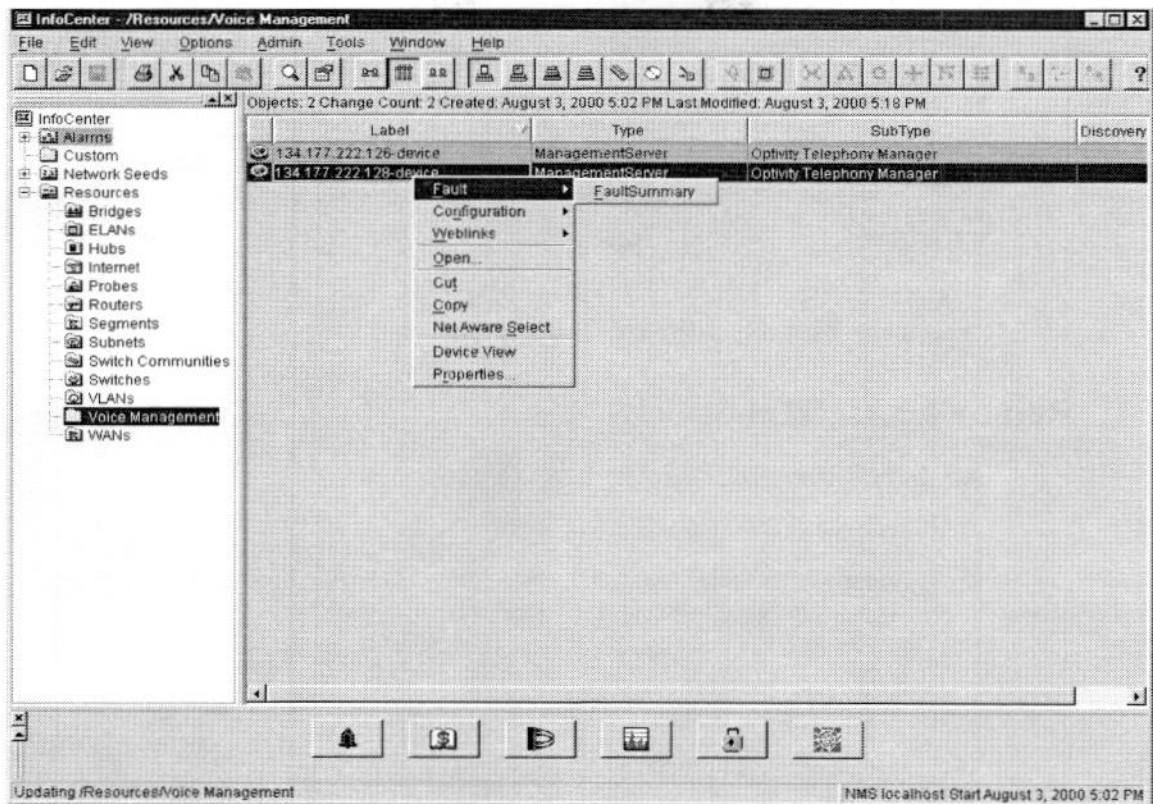
- 1 Select Application Launch from InfoCenter's top menu.
- 2 Select the Fault Summary application (Figure 114).

- 3 While holding down the Ctrl and Shift keys, select the ManagementServer > Optivity Telephony Manager resource to enable FaultSummary for OTM.
- 4 Click Apply.

Figure 114 Modify Application Launch dialog box

To launch FaultSummary:

- ➔ Select the OTM icon and use the right-click menu to launch FaultSummary (Figure 115).

Figure 115 Launch FaultSummary

Configuring OTM

The Optivity Telephony Manager Server must be set up to forward traps to Optivity NMS. Forwarded traps must be in the OTM Open Alarm II format to be recognized.

The OTM Alarm notification application forwards traps of interest to Optivity NMS.

Sample scripts are provided with the Alarm Notification application, which you can modify in the following ways to forward traps:

- Change the target IP to the address of the Optivity NMS Server.

- Select the severity of the traps that you want to forward: Critical, Major, Minor, as so on.
- Modify the sample scripts to forward traps from devices other than Meridian 1, Succession CSE 1000, and other OTM devices to Optivity NMS.



Note: Take care to translate the incoming trap to OTM Open Alarm II, and set the proper device identification and error code fields.

These traps, when received by Optivity NMS, result in a change of status of OTM and can be viewed through the Fault Summary.

Removing an OTM Server

- 1 In InfoCenter, open a folder in the Folders pane.
- 2 Select the OTM Server that you want to delete.
- 3 From the InfoCenter menu bar, choose File > Delete. This action deletes the object from Optivity NMS.

Troubleshooting

If you do not see the OIHOME environment variable, you must manually set it before installing OTM or manually running oitInstall to update the Optivity NMS database.

If you do not see ManagementServer type and Optivity Telephony Manager sub-type on the Device — Add panel:

- Check to see if the OIHOME variable was set.
- Check to see if the OTM OIT files are present and in the correct folder.
- Check the oitInstall log file to verify that the OTM entries were updated.
- You may need to run oitInstall again.

If you cannot see the OTM Server that you have added:

- Check the View Properties of the folder to verify that it can display OTM servers.

If you cannot launch or connect to OTM Web Applications:

- Verify that the IP Address of the OTM Server entered in InfoCenter is correct.
- Verify that the OTM Web Server is running.
- Verify that you have the proper Java Plug-In installed.

If you are not receiving traps from an OTM Server:

- Verify that the OTM Alarm Notification application is running and receiving traps.
- Verify that the OTM Alarm Notification scripts are configured to send traps to Optivity NMS.
- Check the oitInstall log files to verify that the OTM entries were updated.
- Check the status of Optivity NMS daemons from Control Panel > Services, or by typing `optstatus -fe` at the command prompt.

If you cannot launch Fault Summary for OTM:

- Check the Application Launch entries. FaultSummary should be enabled for ManagementServer > Optivity Telephony Manager.

Integrating OTM with HP OpenView

Overview

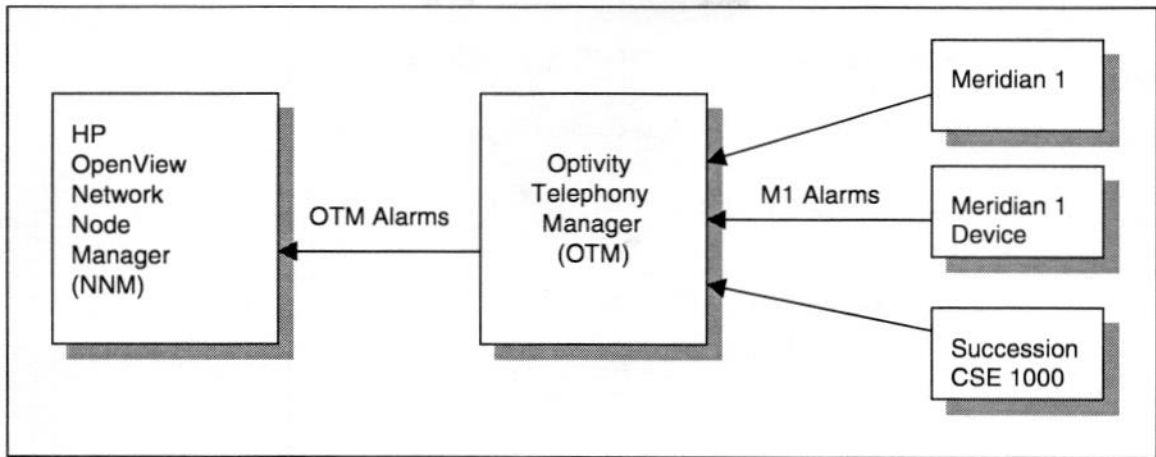
This section provides information on the integration of the HP* OpenView* (HP OV) Network Node Manager (NNM) management platform with Nortel Networks' Optivity Telephony Manager (OTM). It discusses the type of integration supported. The included procedures provide detailed step-by-step instructions on how to configure HP OV NNM to access OTM-related functionalities and information.



Note: Nortel Networks' technical support for this feature is limited to support of the two software files that are distributed with OTM, *OtmOpenAlarms.mib* and *OtmStMon.exe*. These files are compatible with the version of HP OpenView that was current at the time your OTM software was released.

This section describes what you should know about integrating OTM with HP OpenView. It includes the following information:

- "Limitations" on page 225
- "Hardware and software requirements" on page 226
- "System integration" on page 226
- "Installation and configuration" on page 229

Figure 116 OTM alarm integration with HP OpenView Network Node Manager

As seen in Figure 116, Meridian 1 systems, Succession CSE 1000 systems, Meridian Mail, and other M1 devices send their alarms to the OTM server, which can then collect the alarms and forward them to the NNM. The NNM displays the OTM alarms in its Alarm Browser and updates the color of the OTM object in the Network Map to reflect the current status of the OTM server, or the status of the devices the OTM server manages. In addition, you can also configure the NNM to allow the network administrator easy access to the OTM server.



Note: Refer to *Using Optivity Telephony Manager (553-3001-330)* for information on configuring the OTM Server to forward alarms to an external management station.

Limitations

- OTM integration with NNM is supported on HP OV NNM Release 6.x running on the Windows NT platform only.
- Coresidency is not supported for NNM and OTM on the same PC. However, for web clients, if JRE 1.3.1 is loaded in the system and the default web browser is Internet Explorer, both OTM and HP OpenView web applications can be launched simultaneously.
- The OTM Server does not support auto-discovery from NNM.

Hardware and software requirements

PC hardware requirements (HP OV PC)

Please refer to HP OV NNM documentation for details.

PC software requirements (HP OV PC)

- HP OV NNM Release 6.x
- OTM Alarm Integration Package:
 - OTM Alarm MIB (OtmOpenAlarms.mib)
 - OTM Status Monitor (OtmStMon.exe)

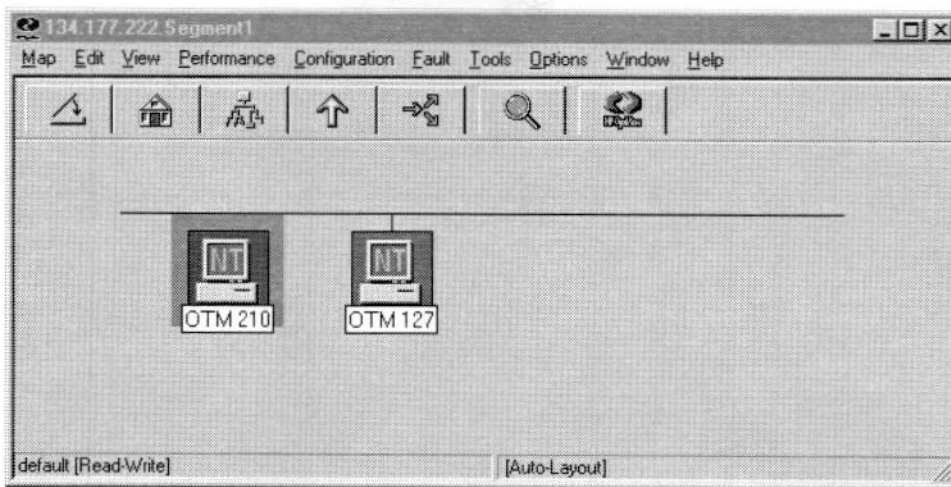
OTM software requirements (OTM PC)

- OTM Release 1.01 or above with:
 - Alarm Notification application
 - Web-based alarm browser

System integration

HP OV NNM Network Map

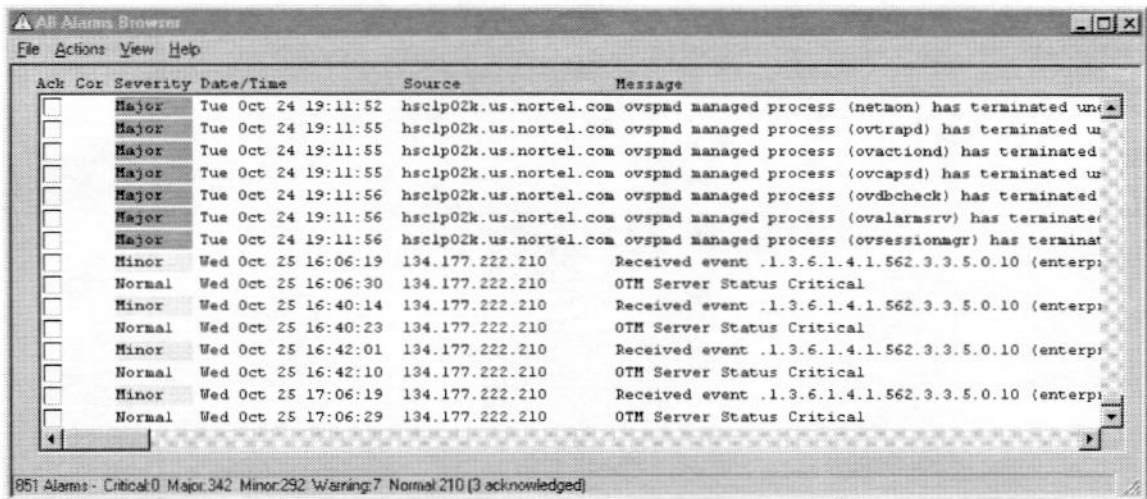
On the NNM Network Map (Figure 117), an OTM server can be represented as an object. You can configure incoming events to trigger a color change to the object icon to indicate the current status of the OTM Server or of the devices monitored by the OTM Server.

Figure 117 HP OpenView Network Node Manager Network Map

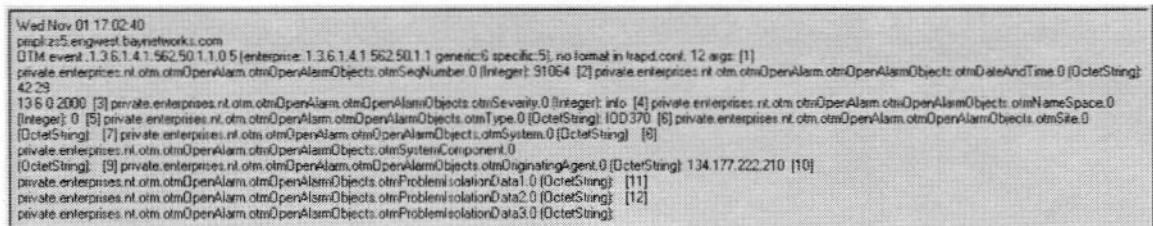
The OTM Status Monitor (OtmStMon) is the program that is used to update the color of the icon for an OTM object. When the color is changed upon the receipt of an incoming event, a message is also logged and appears in the NNM Alarm Browser to indicate the status update.

HP OV NNM Alarm Browser

You can display contents of incoming OTM events in the NNM Alarms Browser (Figure 118).

Figure 118 HP OV NNM Alarms Browser

You can also highlight a specific alarm message on the NNM Alarms Browser, and right-click to display the message content in a separate window (Figure 119). You can then analyze the different variables and their values.

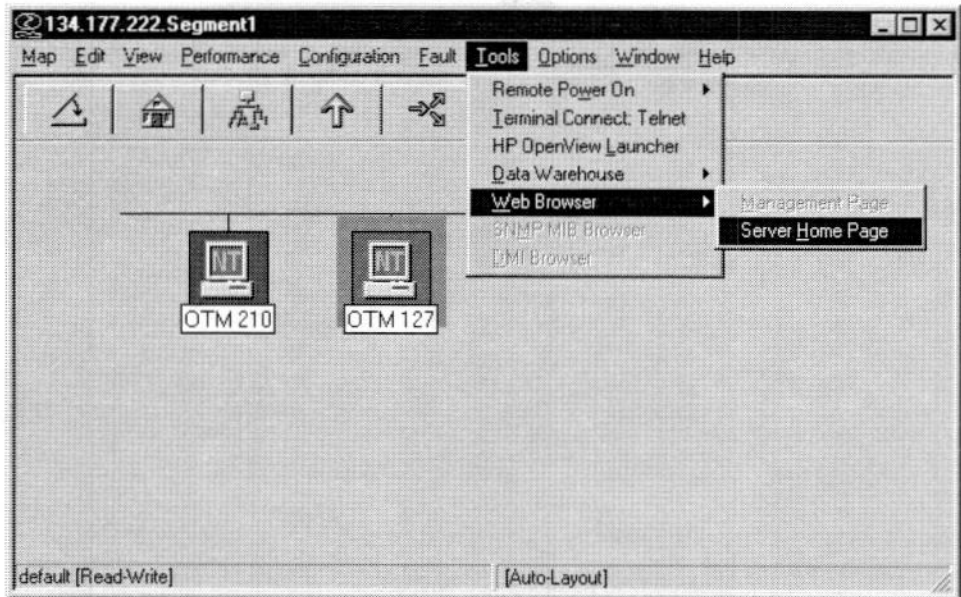
Figure 119 Alarm message content

OTM Web Access

To access the OTM server from NNM:

- 1 Highlight the OTM object on the Network.
- 2 Select Tools > Web Browser > Server Home Page (Figure 120).

Figure 120 OTM Web Access



Your default Web browser is brought up with the Web-based OTM interface. You can log in to the OTM Web Navigator and access the various OTM applications including the OTM Alarm Browser.

Installation and configuration

OTM Alarm Integration Package (HP OV PC)

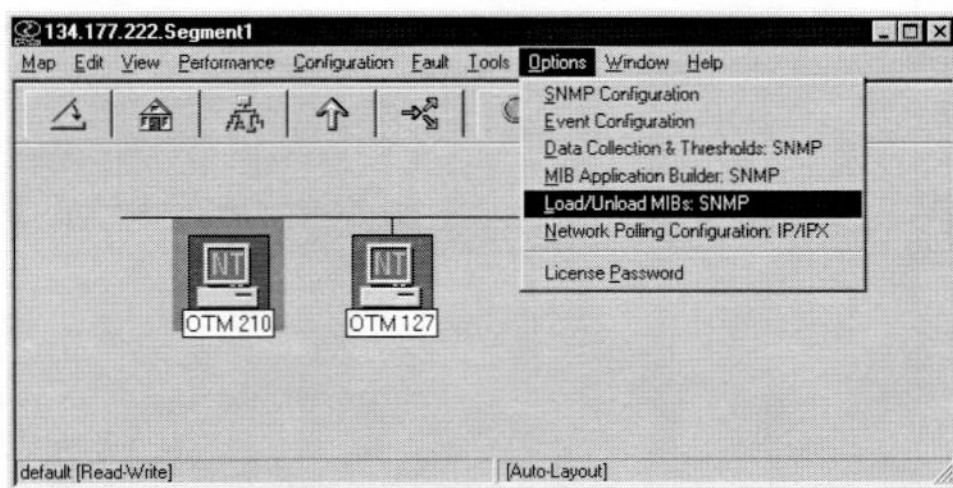
- 1 Copy the OtmStMon.exe to the Openview/bin (\$OV_BIN) directory.
- 2 Copy the OtmOpenAlarms.mib to the directory \$OV_SNMP_MIB/Vendor/NortelNetworks. Create this directory if it does not already exist.

HP OV NNM (HP OV PC)

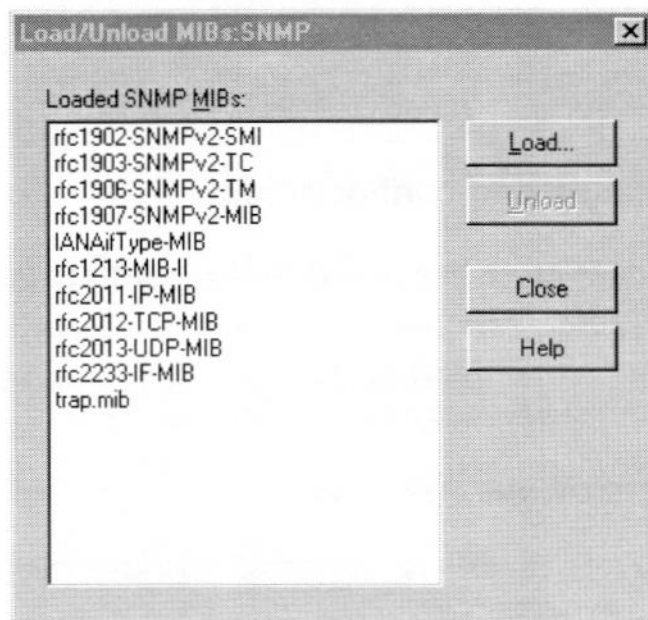
The following configuration procedures are performed while NNM is running:

OTM Alarm MIB installation

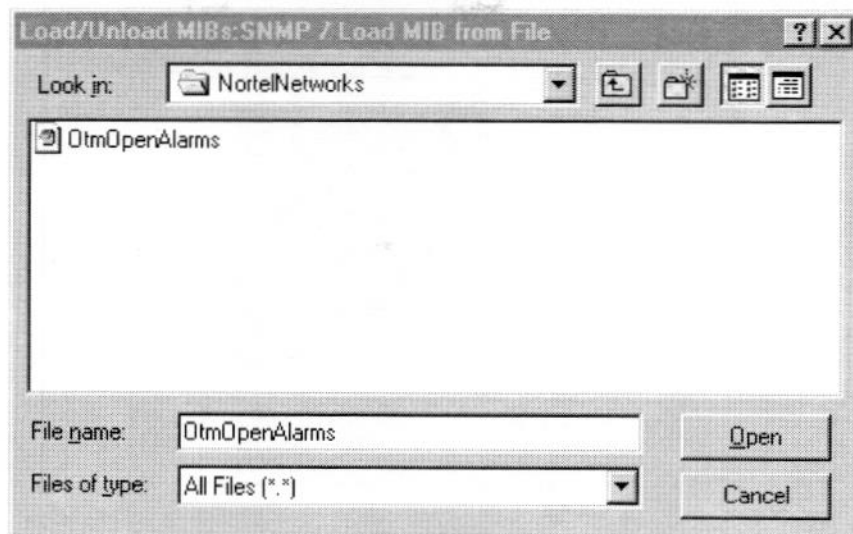
- 1 Select Options > Load/Unload MIBs:SNMP (Figure 121).

Figure 121 NNM Load/Unload MIBs

- 2 Click Load in the Load/Unload MIBs dialog box (Figure 122).

Figure 122 Load/Unload MIBs

- 3 Open the OtmOpenAlarms.mib file (Figure 123).

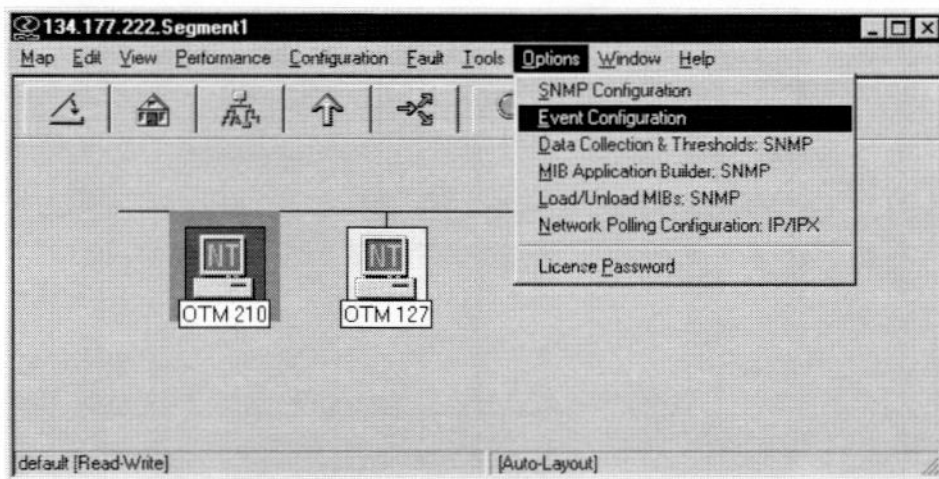
Figure 123 Load MIB

The OTM alarm MIB definitions are now loaded into the NNM's MIB database.

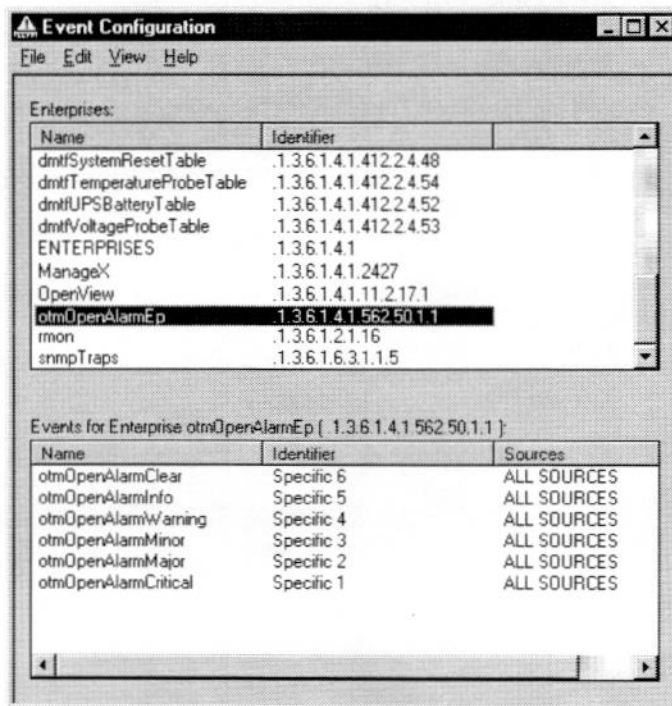
Event Configuration

After the OTM Alarm MIB is loaded, actions must be defined through the NNM Event Configuration for each OTM event.

- 1 Select Options > Event Configuration (Figure 124).

Figure 124 NNM Main Menu - Event Configuration

- 2 Locate and select “otmOpenAlarmEp” from the list of Enterprises (Figure 125).

Figure 125 Event Configuration

There are six events defined for the otmOpenAlarmEp Enterprise. For each event, you configure the desired actions to be taken if the event occurs.

Use the OTM Major Alarm event (otmOpenAlarmMajor, Specific 2) as an example:

- 1 Double-click the corresponding entry on the list.

The Modify Events dialog box appears (Figure 126).

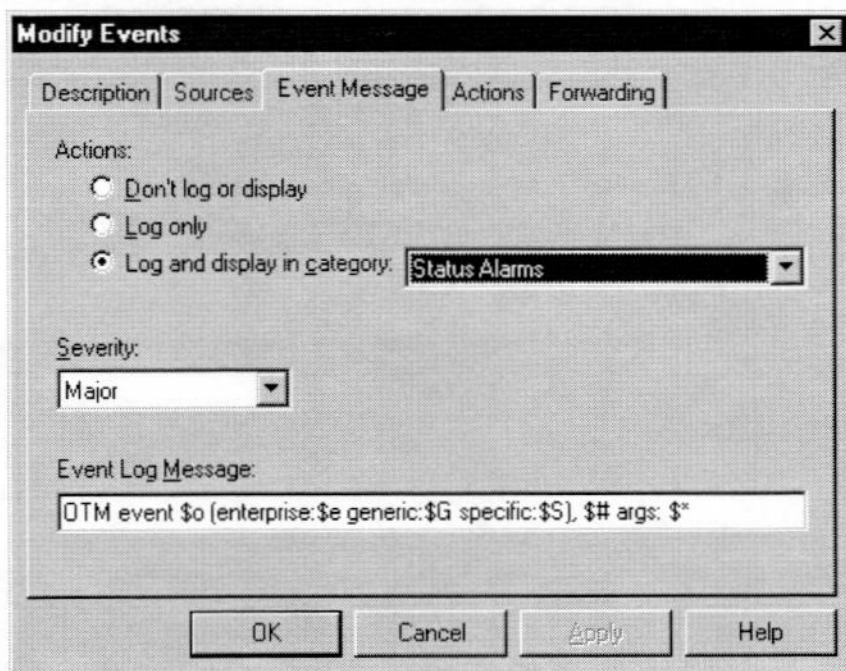
Figure 126 Modify Events - Description

The screenshot shows a 'Modify Events' dialog box with a tabbed interface. The 'Description' tab is selected. The dialog contains the following fields and text:

- Event Name:** otmOpenAlarmMajor
- Enterprise:** otmOpenAlarmEp
- Generic Trap:** Enterprise Specific
- Specific Trap Number:** 2
- Description:**
 - Long Descr.:
" The OTM Open Alarm Trap with a severity of major(2).
This trap is intended to be internationalizable, hence, it contains no natural language text.

At the bottom of the dialog are four buttons: OK, Cancel, Apply, and Help.

- 2 Select the Event Message tab (Figure 127).

Figure 127 Modify Events - Event Message**3** Configure the following:

- a** Actions: Select Log and display in category: Status Alarms.

This enables the display of the incoming event message in the NNM Alarm Browser.

- b** Severity: Select Major for this event.

- c** Event Log Message: Enter the following default text:

OTM event \$o (enterprise:\$e generic:\$G specific:\$S), \$# args: \$*

The displayed message shows the contents of the event message.

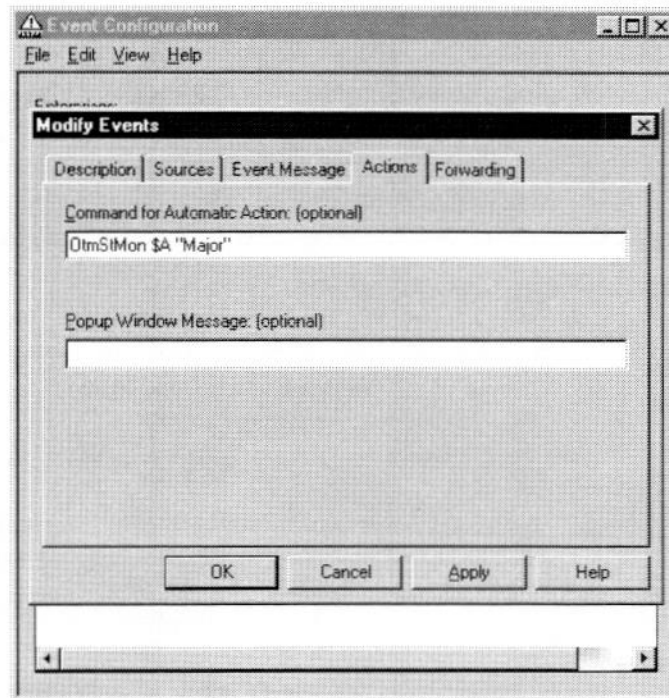


Note: You are allowed to display any message that you choose in the Alarm Browser.

Table 8 Legend for \$ variables in the Event Log Message

Variable	Action
\$o	Print the name (object identifier) of the received event as a string of numbers.
\$e	Print the trap enterprise as an Object ID string of numbers. This number is implied by the event object identifier for non-SNMPv1 events.
\$G	Print the trap's generic-trap number. This number is implied by the event object identifier for non-SNMPv1 events.
\$S	Print the trap's specific-trap number. This number is implied by the event object identifier for non-SNMPv1 events.
\$#	Print the number of attributes in the event.
\$*	Print all the attributes as <i>seq</i> name (type): value strings, where <i>seq</i> is the attribute sequence number.

If you also want the color of the object on the map to change to reflect the occurrence of the incoming event, you can also invoke the OTM Status Monitor (OtmStMon.exe) by specifying a call to it under the "Actions" item (Figure 128).

Figure 128 Modify Events - Actions

OTM Status Monitor

The OTM Status Monitor enables you to change the color of the OTM object on the Network Map to reflect the current status of the server. In addition, a message is also logged onto the HP OV NNM Alarm Browser to indicate the status change.

OtmStMon is written in C and makes use of the HP OV ovevent application. OtmStMon takes in two parameters: an object's selection name and a textual representation of the new status (for example, Critical or Normal). If ovevent cannot locate an object on the current Network Map with the specified selection name, an error message appears. Therefore, if an OTM object is not defined in the Network Map, OtmStMon should not be invoked for an event.

The invocation format for OtmStMon is as follows:

OtmStMon <selection_name> <object_status>

where

<selection_name> is HP OV NNM's unique selection name for an object item on the Network Map

<object_status> is one of the following textual strings: Unknown, Normal, Warning, Minor, Major, Critical, Restricted, Testing, Disabled, Managed, Unmanaged.

If the OTM Status Monitor is not called, then the color of the object that appears on the Network Map does not change for the incoming event.



Note: If no object is defined for the OTM Server on the Network Map, a call to OTM Status Monitor results in an error. Therefore, do not specify calls to OtmStMon if there is no OTM Server defined on the Map.



Note: A call to the OTM Status Monitor results in a message, in addition to the original incoming event message, appearing in the NNM All Alarms Browser (Figure 129). This message is logged whenever the OTM Status Monitor changes the color of an object.

Figure 129 All Alarms Browser

Ack	Cor	Severity	Date/Time	Source	Message
☐		Normal	Mon Oct 30 16:43:33	papkzs5.engvest.baynetworks.com	OTM event .1.3.6.1.4.1.562.50.1.1.0.5
☐		Normal	Mon Oct 30 16:43:33	papkzs5.engvest.baynetworks.com	OTM Server Status Minor
☐		Normal	Mon Oct 30 16:43:38	papkzs5.engvest.baynetworks.com	OTM event .1.3.6.1.4.1.562.50.1.1.0.5
☐		Normal	Mon Oct 30 16:43:38	papkzs5.engvest.baynetworks.com	OTM Server Status Minor
☐		Normal	Mon Oct 30 16:47:09	papkzs5.engvest.baynetworks.com	OTM event .1.3.6.1.4.1.562.50.1.1.0.5
☐		Normal	Mon Oct 30 16:47:09	papkzs5.engvest.baynetworks.com	OTM Server Status Minor
☐		Normal	Mon Oct 30 17:33:00	papkzs5.engvest.baynetworks.com	OTM event .1.3.6.1.4.1.562.50.1.1.0.5
☐		Normal	Mon Oct 30 17:33:00	papkzs5.engvest.baynetworks.com	OTM Server Status Minor

70 of 965 Alarms - Critical:1 Major:3 Minor:0 Warning:0 Normal:66 (3 acknowledged) Filters: Source



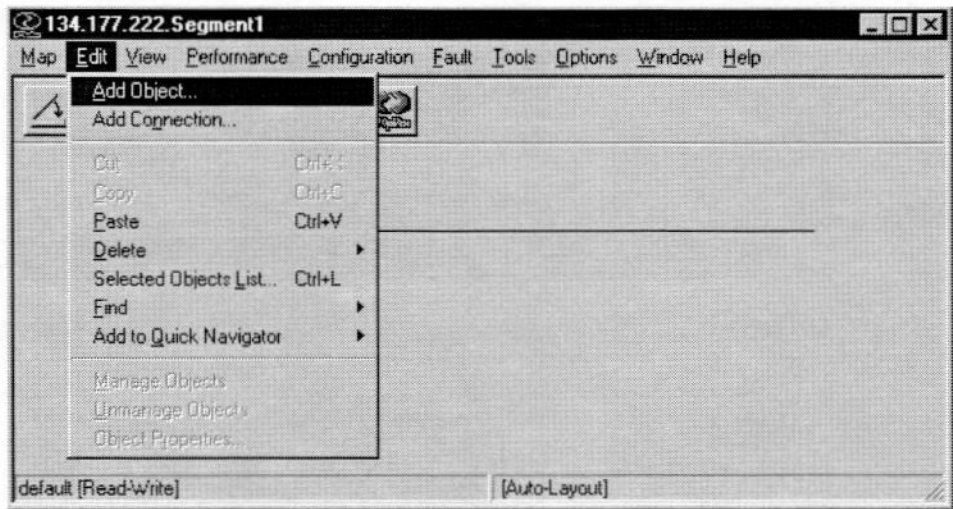
Note: Not every incoming OTM event necessitates the changing of the object's color. For example, a minor or info event may not need to alert the customer. In these cases, the customer may want to configure these events in such a way to simply log the incoming event message and not call OtmStMon.

Network Map set up

To set up an OTM Server object on the Network Map:

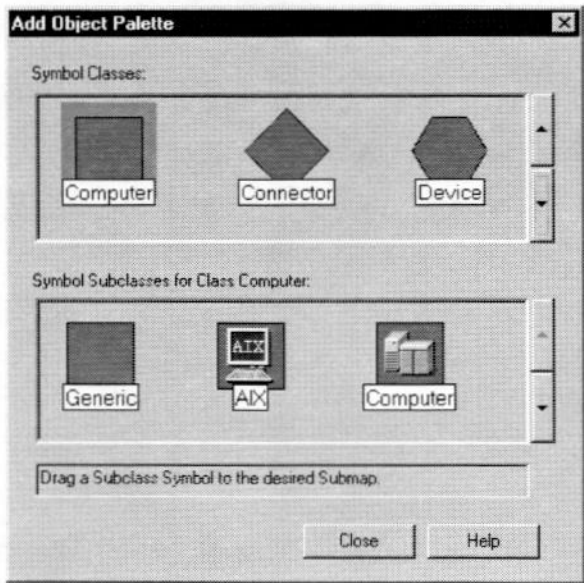
- 1 Locate the appropriate place in the Network Map for the OTM Server.
- 2 Select Edit > Add Object (Figure 130).

Figure 130 NNM Edit - Add Object

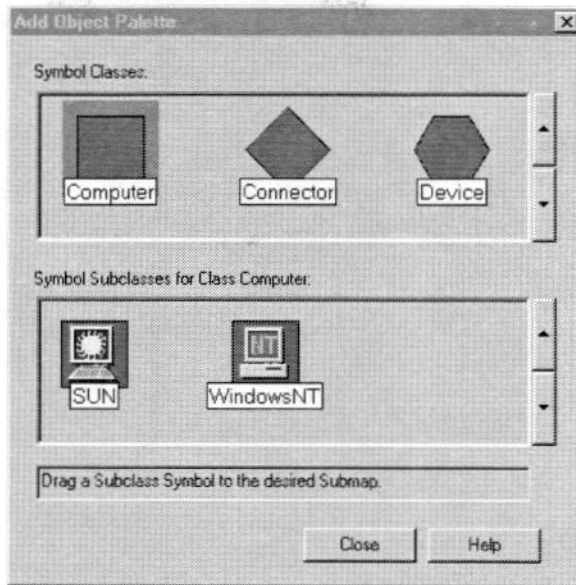


- 3 Select Computer from the Symbol Classes in the Add Object Palette dialog box (Figure 131).

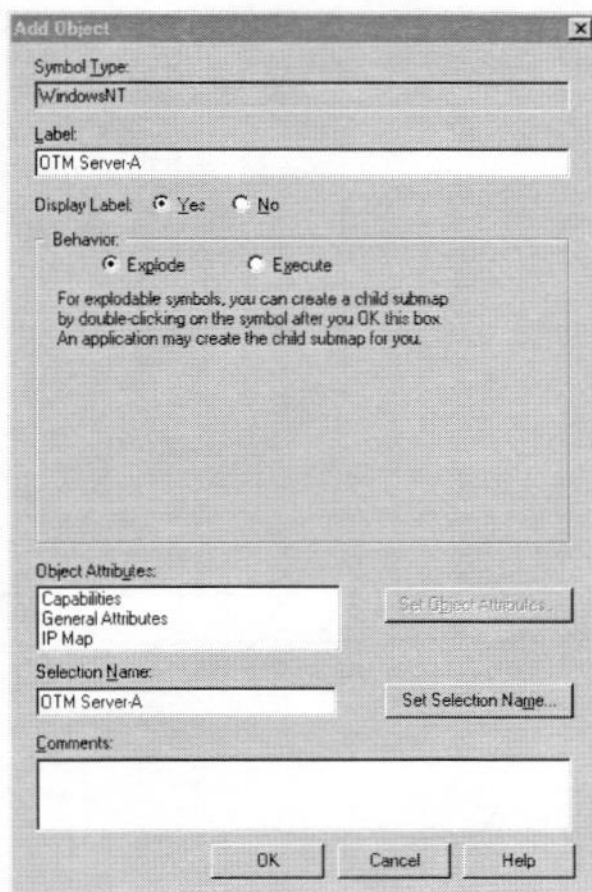
Figure 131 Add Object Palette dialog box



- 4 Select and drag the standard WindowsNT icon from the Symbol Subclasses (Figure 132) onto the appropriate location on the Network Map.

Figure 132 Add Object Palette dialog box II

- 5 The Add Object dialog box opens. Fill in the Label field (OTM Server-A in this example) (Figure 133).

Figure 133 Add Object dialog box

The 'Add Object' dialog box contains the following fields and controls:

- Symbol Type:** A text field containing 'WindowsNT'.
- Label:** A text field containing 'OTM Server-A'.
- Display Label:** Radio buttons for 'Yes' (selected) and 'No'.
- Behavior:** Radio buttons for 'Explode' (selected) and 'Execute'.
- Help text:** 'For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.'
- Object Attributes:** A list box with 'Capabilities', 'General Attributes', and 'IP Map' (selected).
- Set Object attributes...:** A button next to the Object Attributes list box.
- Selection Name:** A text field containing 'OTM Server-A'.
- Set Selection Name...:** A button next to the Selection Name text field.
- Comments:** An empty text area.
- Buttons:** 'OK', 'Cancel', and 'Help' at the bottom.

- 6 Select IP Map under Object Attributes, and click Set Object Attributes (Figure 134).

Figure 134 Add Object - IP Map

The 'Add Object' dialog box is shown with the following fields and options:

- Symbol Type:** WindowsNT
- Label:** OTM Server-A
- Display Label:** ☒ Yes ☐ No
- Behavior:** ☒ Explode ☐ Explode
- Object Attributes:**
 - Capabilities: [Empty]
 - General Attributes: IP Map
- Selection Name:** OTM Server-A
- Comments:** [Empty text area]

Buttons at the bottom: OK, Cancel, Help.

- 7 Select and fill in the entries for Hostname, IP Address, and Subnet Mask (Figure 135).

Figure 135 Add Object - Set Attributes dialog box

- 8** Click OK. You are returned to the Add Object dialog box. In the Selection Name field, enter the same value as that of the Hostname in the previous step (pmpkzs5.engwest.baynetworks.com in this example) (Figure 136).

Figure 136 Add Object - Selection Name

Add Object

Symbol Type:
w/WindowsNT

Label:
OTM Server A

Display Label: ☒ Yes ☐ No

Behavior:
☒ Explode ☐ Explode
 For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

Object Attributes:
 Capabilities
 General Attributes
IP Map

Selection Name:
pmph.zt5.engwest.baynetworks.com

Comments:

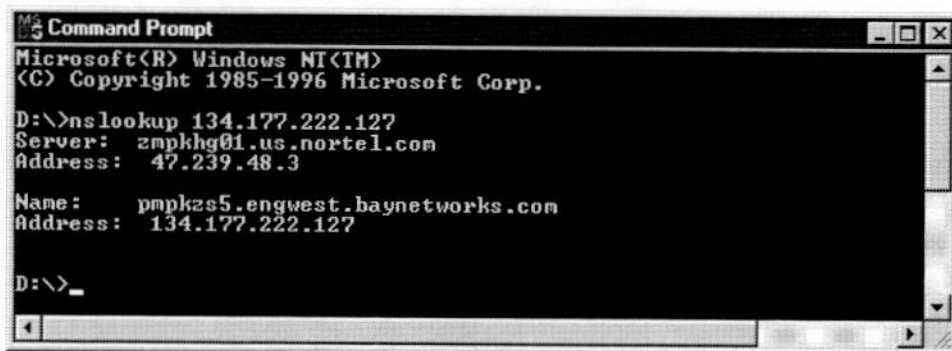
Set Object Attributes... Set Selection Name...

OK Cancel Help

9 Click OK. The object is created on the Network Map.



Warning: The value for Hostname must be the domain name server (DNS) representation of the IP address (if the IP address can be resolved locally). Use the command `nslookup` to retrieve the DNS representation if you do not already know it (Figure 137). If the IP address cannot be interpreted locally, then enter the dotted decimal representation.

Figure 137 nslookup command

- 10 If you want to indicate the status of the OTM Server through the color of the object on the map, be sure to set the Status Source under Symbol Properties to Object (Figure 138, Figure 139).

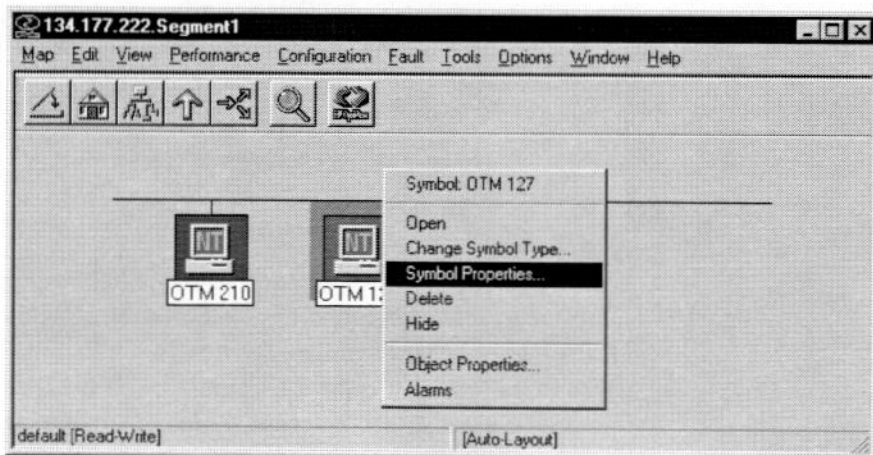
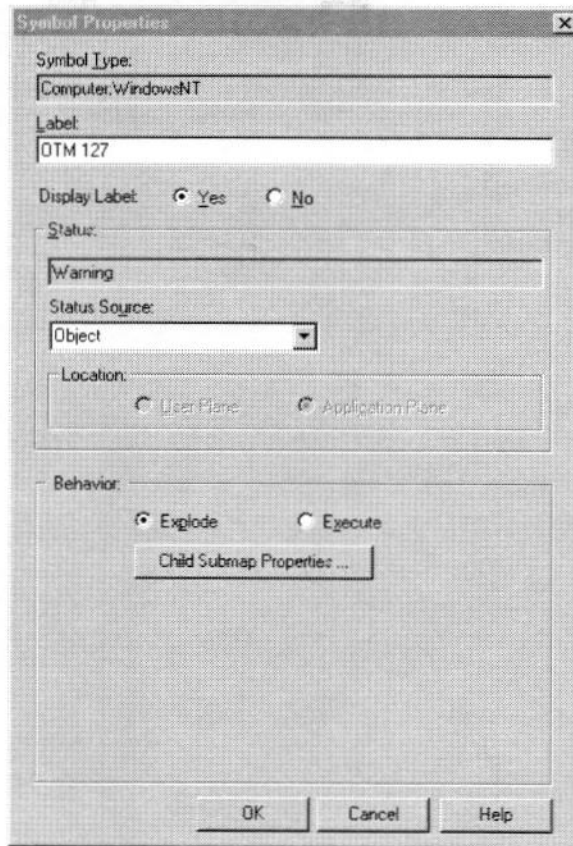
Figure 138 NNM Main Menu - Symbol Properties

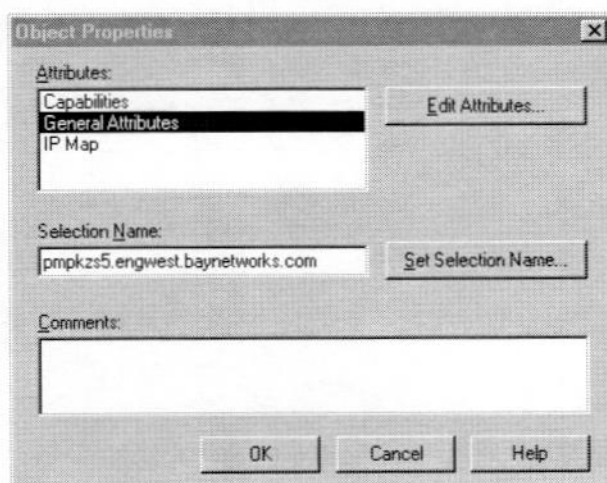
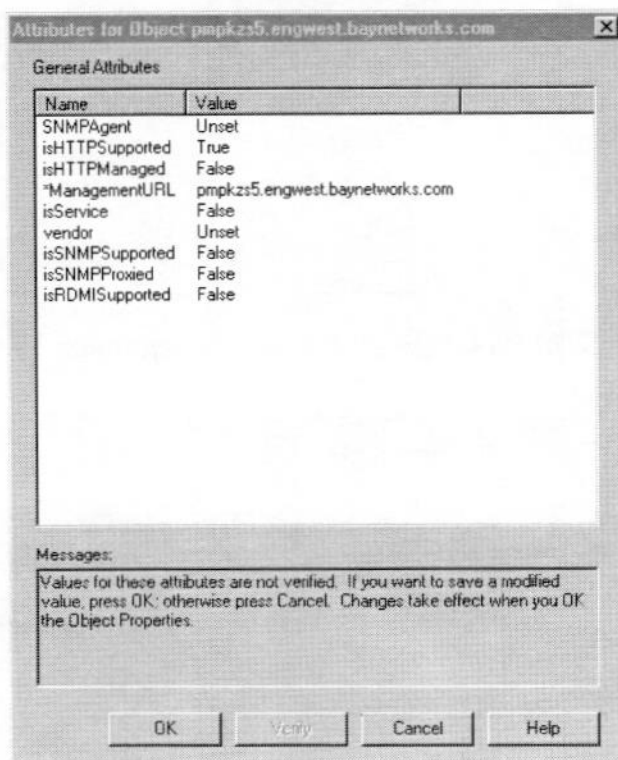
Figure 139 Symbol Properties dialog box

OTM Web Server Access configuration

You can also configure the Management URL to access the OTM Server (Figure 140, Figure 141).

For an object on the Network Map, under General Attributes in the Object Properties dialog box:

- 1 Enter the address (IP address or the DNS name) of the OTM Server in the ManagementURL field.
- 2 Set isHTTPSupported to True.

Figure 140 Object Properties dialog box**Figure 141** Attributes for Object dialog box

OTM configuration (OTM PC)

Refer to the Alarm Management chapter in *Using Optivity Telephony Manager* (553-3001-330) for information on configuring the OTM server to forward SNMP traps to HP OV NNM or other remote systems.

Chapter 3

Windows NT and Windows 2000 reference

This chapter provides reference information related to the Windows NT and Windows 2000 operating systems. The following topics are presented:

- “Installing Windows NT” next
- “Installing Windows 2000” on page 260
- “Testing network cards” on page 266

Installing Windows NT

This section describes an example of Windows NT installation. Due to hardware and software differences, this example may not match your installation.

If a certain component is already correctly installed, then skip the installation of that component.

- “Running the Windows NT setup program” on page 250
- “Installing Windows NT components” on page 251
- “Installing Network Adapter software” on page 252
- “Configuring TCP/IP” on page 253
- “Configuring Initial Workgroups” on page 254
- “Configuring system settings” on page 255
- “Creating an Emergency Repair disk” on page 255
- “Completing the Windows NT installation” on page 255
- “Installing Remote Access Service on Windows NT” on page 256

Hardware compatibility check

Check all hardware against the “Windows NT Hardware Compatibility List” in *Microsoft Windows NT Server Basic and Installation*, and make sure you have all necessary and latest drivers from the manufacturers. For more details, refer to *Microsoft Windows NT Server Basic and Installation, Chapters 5 through 8*. For NT Workstation, refer to *Microsoft Windows NT Workstation Installation Guide, Chapter 1*.

Running the Windows NT setup program



Note: Make sure the first bootup option on CD-ROM in the BIOS is enabled. The installation below requires a server with HDD using a SCSI controller card or a system with RAID. You must get the latest HDD controller from the Manufacturer. For details, check with your server manufacturer.

- 1 Insert the Windows NT server setup CD-ROM into the CD-ROM drive.
- 2 Boot the system.
- 3 On Windows NT Server computers, press F6 immediately when Window NT Setup comes up.
- 4 You see “Setup could not determine the type of one or more mass storage devices... .” Press S.
- 5 You see the Windows NT Setup dialog box. Press Enter to continue.
- 6 Insert the manufacturer-supplied hardware support disk (Hard Disk controller or RAID controller driver) into a: or CD-ROM. Press Enter when ready.
- 7 Select the appropriate driver from the list and press Enter.
- 8 Press Enter if no additional mass storage devices exist.
- 9 In the Windows NT server setup menu, Welcome to Setup, press Enter to set up Windows NT.
- 10 In the Windows NT Server Setup dialog box, you see “Windows NT has recognized the following mass storage... .” Press Enter.
- 11 In the Windows NT Licensing Agreement, press Page Down and choose F8.

- 12 You see "Setup has determined that your computer contains the following hardware and software components." Press Enter to select "The above list matches my computer."
- 13 Press C to create a partition, and type the size of partition you want. The largest size boot partition that you can create is 4095 MB. If the system was previously configured as an NT Workstation, select N for new.
- 14 Select "Unpartitioned Space" on the first disk in the list. (Use the up/down arrow key).
- 15 Press Enter to select "Install Windows NT on the unpartitioned space."
- 16 Use the down arrow key to select "Format partition using the NTFS file system" for the Windows NT partition. NTFS allows management of file security using directory and file permissions. For more details, refer to *Microsoft Windows NT Server Concepts and Planning, Chapter 4*.



Note: The disk format takes approximately 3 minutes for a 4 G drive and only a few seconds on a drive controlled by a RAID controller.

- 17 The default Winnt is prompted. You may change the name or location as you want.
- 18 Press Enter to allow Setup to perform an exhaustive secondary examination of the hard disk.
- 19 Insert the Manufacturer SCSI or RAID driver disk, if applicable, when using a server computer or RAID controller. Press Enter to allow the system to copy the files on the disk.
- 20 Eject the CD-ROM and remove any floppy disk from the floppy drive. Press Enter to reboot the system. At this point, you have finished the first part of Windows NT installation. The computer will be rebooted twice. The second reboot is to convert from FAT to NTFS on the partition in which Windows NT was installed.

When the system reboots, press F2 to instruct the system to boot from the hard drive instead of the CD-ROM.

Installing Windows NT components

- 1 When the Windows NT Setup dialog box appears, click Next on "Gathering information about your computer."

- 2 Enter your Name and Organization Name, and then click Next.
- 3 Enter the information on Licensing Modes. Click Next.
- 4 Enter the unique Computer Name.
- 5 Select the server type on the Server Type dialog box (StandAlone Server is highly recommended).
- 6 Enter the password for the Local Administrator.
- 7 Create an Emergency Repair Disk.
- 8 Select Components, and then Click Next.



Note: Do not use open GL screen savers, which use too much processing time.

Installing Network Adapter software

Before configuring the network adapters, make sure that the adapters are inserted properly into the slots and RJ45 cables are plugged into the adapters. The CLAN card is recommended to install on the top PCI slot and ELAN on the second-from-the-top PCI slot.

- 1 In Windows NT Setup, verify that the Wired to the network check box is checked, and then click Next.
- 2 In the Install Microsoft Internet Information Server dialog box, uncheck the box, and then click Next.
- 3 Click Select from the List in the Network Adapter dialog box.
- 4 Click Have Disk and insert the floppy disk or CD from the manufacturer (shipped with the network card). Click OK and select the appropriate driver from the list. Click OK to continue.
- 5 The next widow displays your LAN card. Since the server has two LAN cards, click on Select from the list to install the CLAN card driver, and follow the previous step to install the CLAN card.
- 6 In the Network Protocol dialog box, only select TCP/IP protocol, and then click Next to continue.
- 7 In the Network Services dialog box, you see the following services:

- RPC configuration
- NetBIOS Interface
- Workstation
- Server

Click to select the desired services.

- 8 Click Next to install selected components.
- 9 Click OK for Adapter Properties.
- 10 If the ELAN card is the same type as the previously installed CLAN card, the following message may appear: "A network card of this type is already installed in the system. Do you want to continue?" Select OK.
- 11 The Adapter Properties dialog box appears for the second LAN card. Click OK to continue.

Configuring TCP/IP

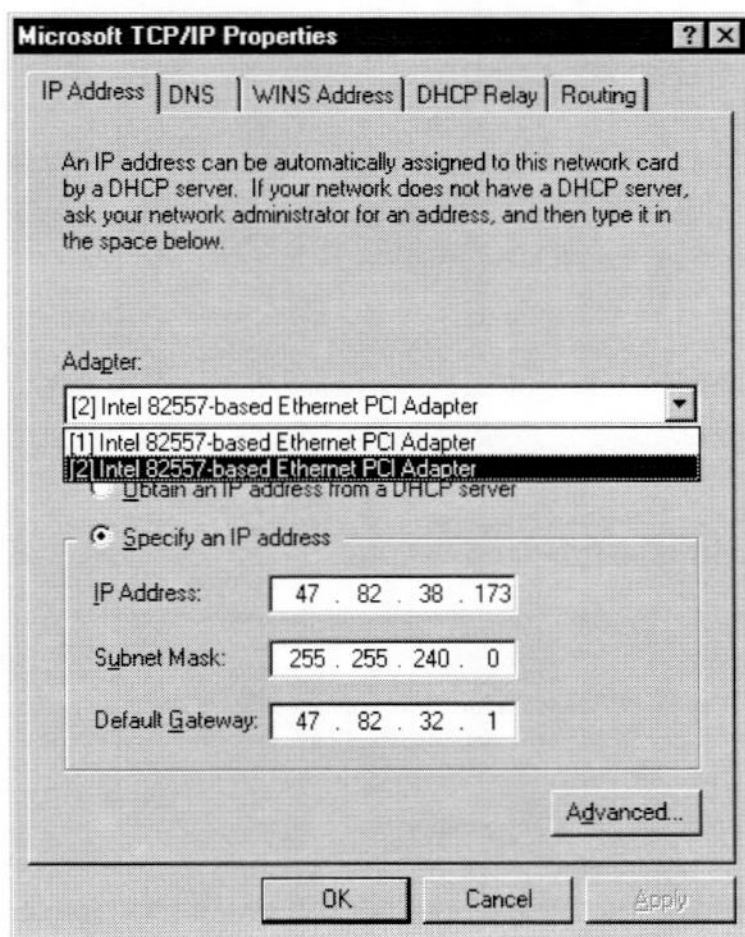
Configure TCP/IP as follows:

- 1 The TCP/IP Setup dialog box appears (Figure 142). If you have a DHCP server and want to configure the IP address from the DHCP server, then select Yes. Otherwise, select No and proceed to the next step.
- 2 In the TCP/IP Configuration dialog box:
 - Select adapter "[1]..." and enter the IP Address, Subnet Mask, and Default Gateway for the Customer LAN (CLAN) connection.
 - Select adapter "[2]..." and enter the IP Address, Subnet Mask, and Default Gateway for the Embedded LAN (ELAN) connection.
 - Click OK to continue.
- 3 In the Show Binding For dialog box, click Next to continue.



Note: For IP routing, the Enable IP Forwarding check box is unchecked by default. Nortel Networks recommends leaving this check box unchecked to avoid security and performance problems.

For more information, refer to Chapter 7 of *Microsoft Windows NT Server Basics and Installation*.

Figure 142 Microsoft TCP/IP Properties dialog box

Configuring Initial Workgroups

- 1 In the Domain / Workgroup Setting dialog box, use the default Workgroup settings and click OK to continue.
- 2 Click Finish in the Finishing Setup dialog box.
- 3 In the Internet Information Server Installation dialog box, remove the gopher selection.
- 4 Install the SQL server driver.

- 5 In the Microsoft Internet Information Server dialog box, click Cancel. The Microsoft Internet Information Server will be installed in Option Pack 4.

Configuring system settings

Configure system settings as follows:

- 1 In the Date/Time Properties dialog box, select your Time Zone.
- 2 Select the check box (default is checked) for automatically adjusting for Daylight Saving Time.
- 3 In the Display Setting dialog box:
 - Select OK to verify that the video adapter was detected.



Note: If you do not have the correct video driver, you must install the correct driver, after reboot, from the manufacturer's diskette.

- Color Palette: # of colors (use default setting)
 - Desktop Area: 1240 by 768 pixels
 - Font Size: Small Fonts
 - Refresh Frequency: (use default setting)
- 4 Click Test, and then click OK to test the display. Save the display settings when prompted (select OK to save). Click OK to exit the Display Settings.

Creating an Emergency Repair disk

In the Emergency Repair disk dialog box, select Yes to create an Emergency repair disk.

Completing the Windows NT installation

Click Restart Computer to reboot the system.

The Windows NT installation is complete.

Installing Remote Access Service on Windows NT

Remote Access Service provides the ability to administer OTM remotely. For more information, refer to Chapter 6 in the *Windows NT Server Network Supplement*.

- 1 Choose Control Panel > Network. Click the Services tab, and then click Add to add Remote Access Service software.
- 2 Insert the Windows NT server CD, and then click Continue.
- 3 Select Yes to “invoke the modem installer to enable you to add a modem.”



Note: A modem does *not* have to be attached to install this software.

- 4 In the Install New Modem dialog box, click Next to continue.
- 5 If the system cannot detect the modem for you, you must insert the manufacturer's disk that comes with the modem, and choose Have Disk to install.
- 6 If the system does not have a modem attached, select Standard 28800 bps Modem from the list.
- 7 In the Selected Port dialog box, select COM1, and then click Next.
- 8 In the Location Information dialog box, enter your Area Code, click Next, and then click Finish.
- 9 A dialog box appears that lists the modem Port, Type and Device.
- 10 Select Configure... to choose “Dial out and Receive Calls” as Port Usage. Click OK.
- 11 Select Network... to configure TCP/IP. Click OK.
- 12 In the RAS Server TCP/IP Configuration dialog box, select This Computer only. Select Use Static Pool, and enter the initial range as 1.0.0.1 to 1.0.0.255. Click OK to return to the Remote Access Setup dialog box and click Continue.
- 13 In the “Remote Access Service has been successfully installed” dialog box, click OK.
- 14 In the Network dialog box, click OK. Click Close.

The system binds all the network protocol software. Remove the Windows NT Server CD, and press Enter to restart your server.

RAS with TCP/IP

With TCP/IP you can allow an incoming call to access only the RAS Server, or you can allow the computer making the incoming call to access the rest of the network as well.



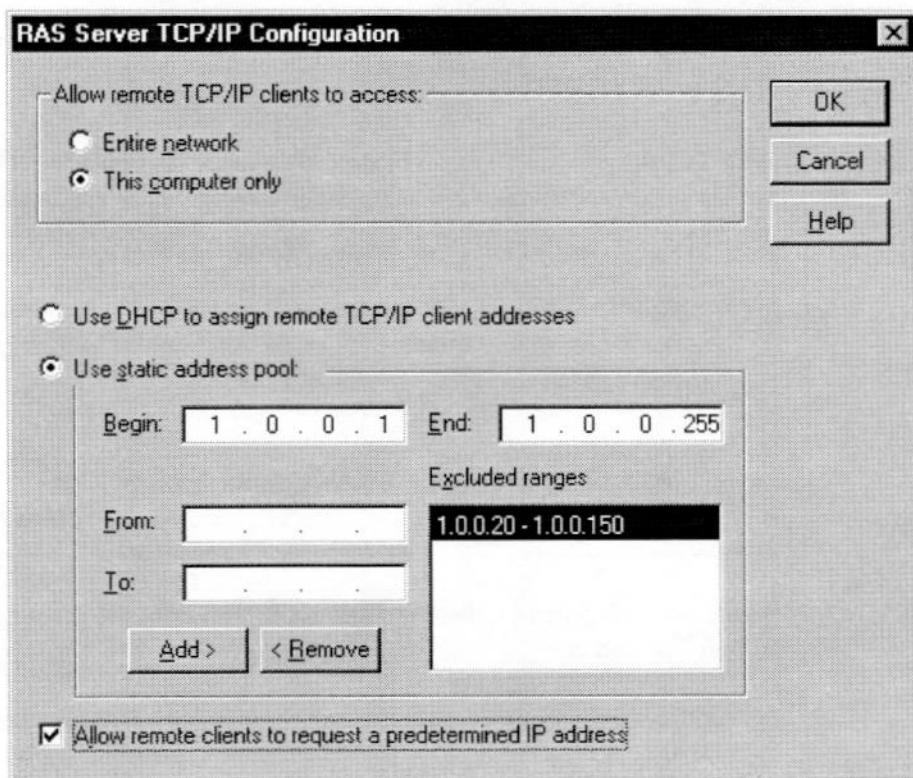
Caution: For security reasons, Nortel Networks recommends allowing the incoming call to access "The computer only," which is the RAS Server itself.



Note: This configuration is only available on Windows NT Server. If you run OTM on a Windows NT Workstation, you do not have this capability.

As shown in Figure 143, there are three configurations for getting the IP address from RAS. You can:

- Configure to get the IP address via Dynamic Host Configuration Protocol (DHCP)
- Configure the IP address to come from a pool of IP addresses maintained on the RAS Server
- Allow the incoming connection to request its own IP address

Figure 143 RAS Server TCP/IP Configuration dialog box

Grant permission

After installing Remote Access software on a server, you must grant Remote Access permission to users.

Callback

As an additional measure of security, the callback feature ensures that only users from specific locations can access the RAS Server. You configure each user's callback privilege when granting Remote Access permission.

Encrypted passwords and data encryption

As shown in Figure 144, the default setting for RAS password authentication is to require Microsoft Encrypted Authentication. When you select this option, Nortel Networks assumes you only use Microsoft clients (Windows 98, Windows NT Server or Workstation, Windows 2000 Server or Professional computers) to connect to the RAS Server.

For additional security, if you use the MS-CHAP protocol, then you can also set the RAS device to require data encryption. This enables data encryption between the RAS Server and client as well as the password exchanged to establish the connection.

Multilink

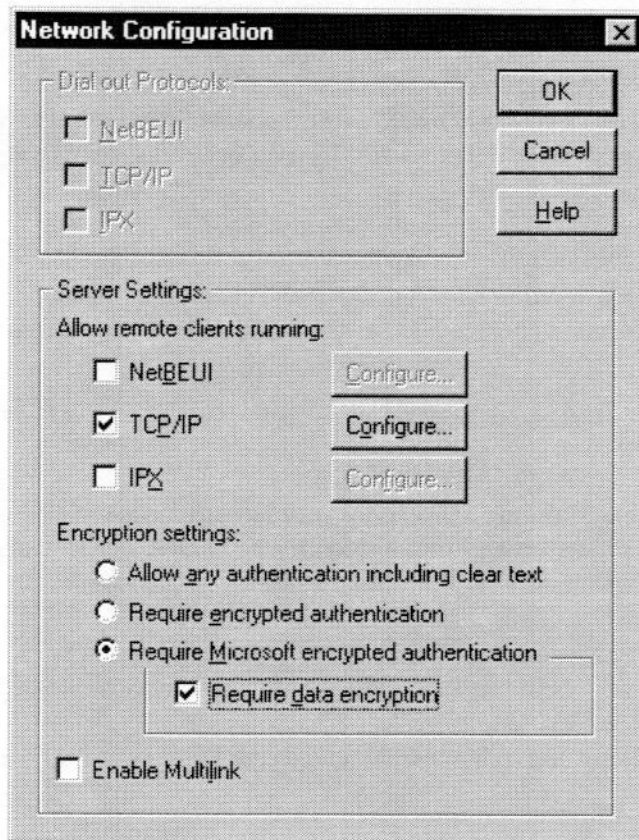
You can enable Multilink to speed up your remote access. Multilink combines multiple serial data streams into one aggregate bundle. For instance, if you have two 56 Kbps modems with Multilink enabled, your bandwidth can be aggregated to 134.4 Kbps.

To use Multilink, both the server and client must have Multilink enabled.

For more information, refer to Chapter 6 in the *Windows NT Server Networking Supplement*.

RAS client

The security you select must match the security selected on the remote server. However, if either side selects "Allow any authentication including clear text," then it does not matter which protocol the other side uses.

Figure 144 Network Configuration dialog box

Note: The data encryption and multilink features are only available on Windows NT Server.

Installing Windows 2000

This section describes an example of Windows 2000 installation. Due to hardware and software differences, this example may not match your installation.

If a certain component is already correctly installed, then skip the installation of that component.

- “Running the Windows 2000 setup program” on page 261
- “Installing Windows 2000 components” on page 262
- “Configuring TCP/IP” on page 263
- “Installing a modem” on page 264
- “Installing Remote Access Service on Windows 2000” on page 264

Hardware compatibility check

Check all hardware against the documentation available on Microsoft’s web site at <http://www.microsoft.com/windows2000/support/online/docs/default.asp>.

Running the Windows 2000 setup program



Note: Make sure the first bootup option on CD-ROM in the BIOS is enabled.

- 1 Insert the Windows 2000 server setup CD-ROM into the CD-ROM drive.
- 2 Boot the system.
- 3 In the Windows 2000 Server Setup Welcome dialog box, press Enter to set up the Windows 2000 Server.
- 4 In the Windows 2000 Licensing Agreement dialog box, press Page Down to go to the bottom of the page, and then choose F8.
- 5 Press C to create a partition, and then type the size of the partition that you want to create.
- 6 Use the up and down arrow keys to select the partition created on the first disk in step 5.
- 7 Press Enter to set up Windows 2000 on the selected item.
- 8 Use the up and down arrow keys to select Format partition using the NTFS files system, and then press Enter.
- 9 Wait while the set up program formats the partition. This will take several minutes.
- 10 Wait while the set up program copies files to the Windows 2000 installation folders. This will take several minutes.

11 Reboot the system.

When the system reboots, press F2 to instruct the system to boot from the hard drive instead of the CD-ROM.

Installing Windows 2000 components

Windows 2000 Server set up continues after the reboot.

- 12** The Installing Devices dialog box appears. This will take several minutes.
- 13** The Regional Settings dialog box appears. Select the default values or configure as needed, and then click Next.
- 14** The Personalize Your Software dialog box appears. Enter your name and the name of your organization, and then click Next.
- 15** The Your Product Key dialog box appears. Enter the product key, and then click Next.
- 16** The Licensing Modes dialog box appears. Select the default value, or choose Per Server or Per Seat, as appropriate, and then click Next.
- 17** The Computer Name and Administrator Password dialog box appears. Enter the computer name and the administrator password, and then click Next.
- 18** The Windows 2000 Components dialog box appears. Select the default values or select specific components, as appropriate, and then click Next.
- 19** The Date and Time Settings dialog box appears. Adjust the Date, Time, and Time Zone, as appropriate, and then click Next.
- 20** Wait for the Network Settings dialog box to appear. This will take several minutes.
- 21** When the Network Settings dialog box appears, accept the default value, Typical Settings, and then click Next.
- 22** The Workgroup or Computer Domain dialog box appears. Make the appropriate selection, and then click Next.
- 23** Wait while the set up program installs components. This will take several minutes.
- 24** Wait while the set up program performs final tasks. This will take several minutes.

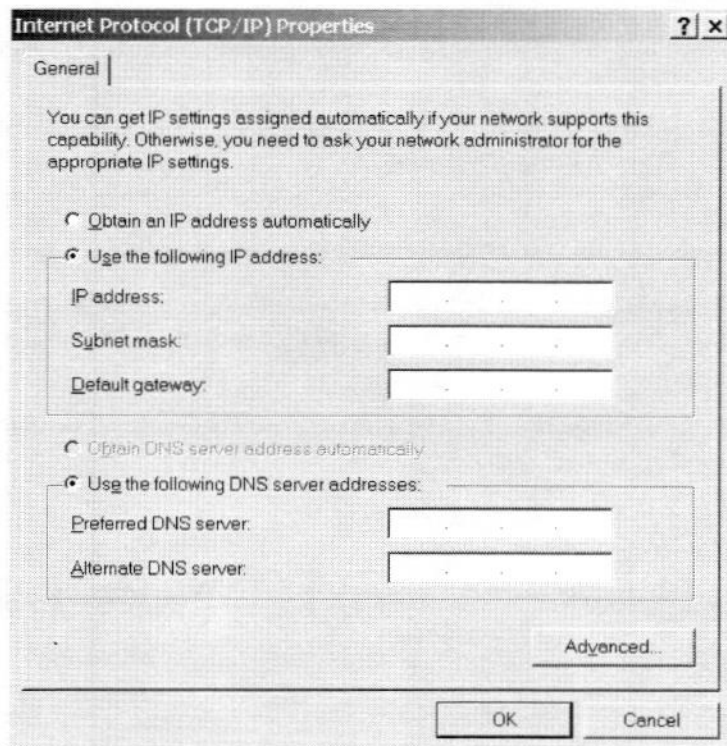
- 25 The Completing the Windows 2000 Setup Wizard dialog box appears. Click Finish to reboot the system.

Configuring TCP/IP

- 1 Choose Start > Settings > Network and Dialup Connections.
- 2 In the Network and Dialup Connections dialog box, right-click the Local Area Connection icon, and then select Properties.
- 3 In the Local Area Connection Properties dialog box, click to select Internet Protocol (TCP/IP), and then click Properties.

The Internet Protocol (TCP/IP) Properties dialog box appears (Figure 145).

Figure 145 Internet Protocol (TCP/IP) Properties dialog box



- 4 If you have a DHCP server and you want to configure the IP address from the DHCP server, click the Obtain an IP address automatically radio button, and go to step 6; otherwise, proceed to the next step.

- 5 Click the Use the following IP address radio button. Enter the IP address, Subnet Mask, Default gateway, and DNS server information.



Note: Click Advanced... in the Internet Protocol (TCP/IP) Properties dialog box to enter WINS server information.

- 6 Click OK, and then reboot the system.

Installing a modem

- 1 Choose Start > Settings > Control Panel.
- 2 Double-click the Phone and Modem Options icon.
- 3 In the Phone and Modem Options dialog box, click the Modems tab.
- 4 If the modem on the computer is not already installed, click Add... .



Note: If it is attached to the computer, Windows 2000 may detect and install a modem automatically.

- 5 In the Install New Modem dialog box, click Next to continue.
- 6 If the system is unable to detect the modem, you must insert the modem manufacturer's disk that came with the modem, and then select Have disk to install.
- 7 If the system does not have a modem attached, select Standard 28800 bps Modem from the list.
- 8 Click Finish to close the dialog box.

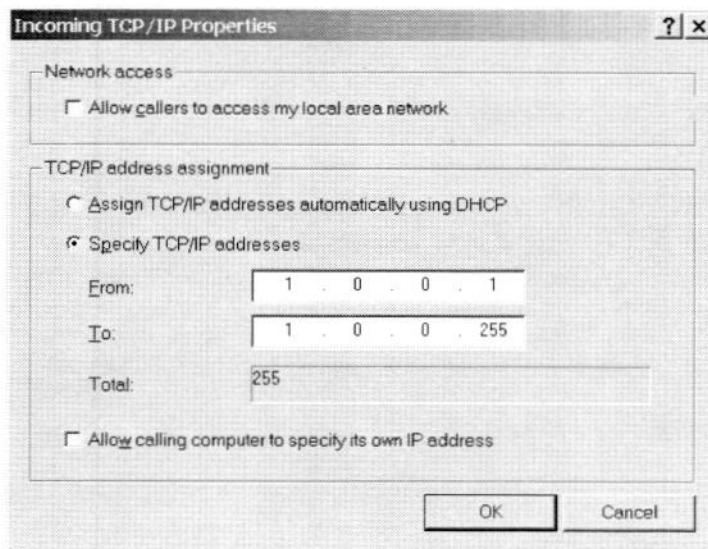
Installing Remote Access Service on Windows 2000

- 1 Choose Start > Settings > Network and Dialup Connections.
- 2 Double-click the Make New Connection icon.
- 3 In the Network Connection Wizard welcome dialog box, click Next.
- 4 In the Network Connection Type dialog box, select Accept incoming connections, and then click Next.

- 5 In the Devices for Incoming Connections dialog box, select the appropriate connection device, and then click Next.
- 6 In the Incoming Virtual Private Connection dialog box, check the Do not allow virtual private connections check box, and then click Next.
- 7 In the Allowed Users dialog box, select the users that are allowed to connect to the server, and then click Next.
- 8 In the Networking Components dialog box, click to select Internet Protocol (TCP/IP), and then click Properties.

The Incoming TCP/IP Properties dialog box appears (Figure 146).

Figure 146 Incoming TCP/IP Properties dialog box



- 9 In the Incoming TCP/IP Properties dialog box, uncheck the Allow callers to access my local area network check box. Click the Specify TCP/IP address radio button. Enter the initial range as From 1 . 0 . 0 . 1 To 1 . 0 . 0 . 255, and then click OK.
- 10 In the Networking Components dialog box, click Next.
- 11 In the Completing the Network Connection Wizard dialog box, type the connection name, and then click Finish.

Testing network cards

Test the network cards after you complete the Windows NT or Windows 2000 installation.

Testing the Customer LAN

- 1 Configure the Captive Client IP address on the same subnet as the Customer LAN (CLAN). The equivalent subnet would be the BINARY AND of the full Captive Client IP address with the CLAN subnet mask (for example, 255.255.240.0). The subnet mask of the Captive Client would be the same as that for the CLAN.
- 2 Ping the CLAN IP Address from Captive Client (for example, 47.82.38.100).

Testing the Embedded LAN

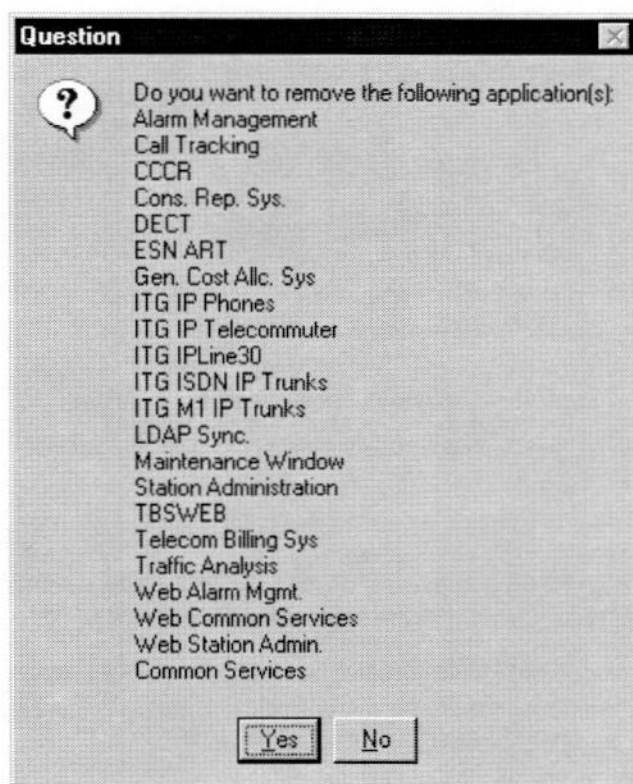
- 1 Configure the Captive Client IP address on the same subnet as the Embedded LAN (ELAN). The equivalent subnet would be the BINARY AND of the full Captive Client IP address with the ELAN subnet mask (for example, 255.255.240.0). The subnet mask of the Captive Client is the same as that for the ELAN.
- 2 Ping the ELAN Address from Captive Client (for example, 47.114.45.3).

Chapter 4

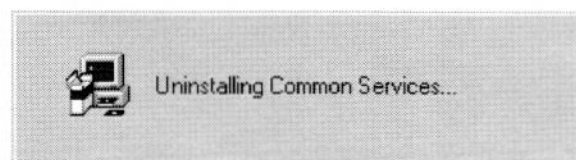
Uninstall OTM

Use Uninstall to remove software that is no longer needed, or that has become damaged or was incorrectly installed.

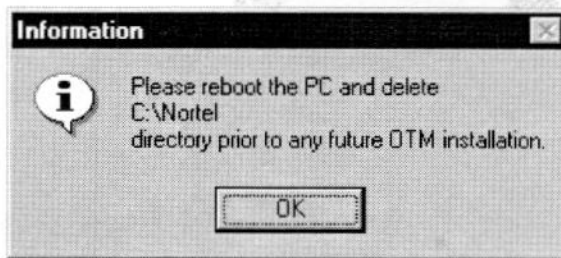
- 1** Use one of the following two methods to access Uninstall:
 - a** From the Start menu, select Programs > Optivity Telephony Manager > OTM Uninstaller.
 - or
 - b** In the Software Installation Wizard, select Uninstall in the Setup Choices dialog box. See “Setup Choices” on page 48.
- 2** The Uninstall Confirmation dialog box (Figure 147) displays a list of the OTM applications that are currently installed, and asks for confirmation that you want to delete them. Click Yes to continue.

Figure 147 Uninstall Confirmation dialog box

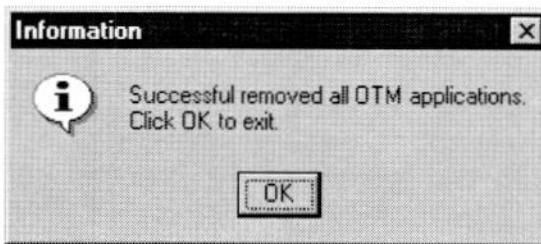
- 3** The status box (Figure 148) provides a visual indicator of the progress of the uninstall process. Common Services is the last application to be uninstalled.

Figure 148 Uninstall status box

- 4** The Reboot request dialog box appears requesting that you reboot the PC and reminding you to delete the OTM directory (Figure 149). Click OK to continue.

Figure 149 Reboot request dialog box

- 5 The Uninstall complete dialog box appears indicating that all OTM applications have been removed (Figure 150). Click OK to exit.

Figure 150 Uninstall complete dialog box

Reboot the PC and remove the directory where the OTM software was installed.

Appendix A

OTM engineering guidelines

This appendix provides a set of guidelines to help you determine the configuration and distribution of OTM servers within a network to efficiently manage Meridian 1 and Succession CSE 1000 systems.

This appendix includes the following sections:

- “Capacity factors” next
- “Software limits” on page A-3
- “Operational limits” on page A-8
- “PC hardware” on page A-11
- “Network bandwidth” on page A-18
- “OTM System Performance” on page A-24
- “OTM port usage” on page A-34
- “Sample walk-through of computations” on page A-36

Capacity factors

This appendix examines the following areas where capacity is a factor:



Note: Analysis was performed on the majority of OTM features. To simplify analysis, only those features that impact these resources are highlighted here.

- Features running on the OTM Server and their impact to its resources, such as CPU usage, physical memory (RAM), and disk storage
- Web and OTM Clients and their impact on OTM Server resources

- Web-based Station Administration Write capability (that is, performing Station updates over the Web) and its impact on the OTM Server
- Meridian 1 and Succession CSE 1000 and their impact on OTM Server resources
- Communications between the OTM Server and Meridian 1 systems, Succession CSE 1000 systems, OTM/Web Clients, LDAP Server, and so on, and their impact on the network to which they are connected



Note: The Billing applications result in a processor load that is not possible to predict. The exact impact depends on several factors, including types of reports being generated and quantity of data being merged. It is not possible to derive a general formula to predict the impact of these applications. Nortel Networks recommends that these applications be run during off-hours, and that they not be run in parallel with other resource-intensive applications.

Based upon this analysis, recommendations are made as to:

- The resources required on the OTM Server
- The number of Clients and Meridian 1 or Succession CSE 1000 systems that can be connected to a single OTM Server
- Network bandwidth and routing considerations

Analysis of the results of benchmark testing are presented in Table A-3 on page A-11, Table A-5 on page A-22, and Figure A-5 on page A-25. The tables can be used to calculate the resources and connections possible for various OTM Server usage scenarios.

- Table A-3 highlights PC performance for several OTM applications.
- Table A-5 highlights the peak and average transfer rates for various OTM activities.
- Figure A-5 presents a graphical representation of station response time compared with round trip time (RTT).

To aid in this process, this appendix analyzes four typical OTM Server configurations. Use these configurations as examples and the raw table data to extrapolate configurations specific to a given customer/distributor setup.

These guidelines provide minimum PC configurations for the OTM Server, OTM Client, Web Client, and OTM running in a stand-alone mode. The resource calculations presented herein are centered around the OTM Server running on a Windows NT Server Platform.

Table A-4 on page A-17 lists the limitations of running the OTM Server on a Windows NT Workstation; however, the analysis presented here does not cover this platform.



Note: OTM running in a stand-alone mode functions in a manner that provides access to Meridian Administration Tools (MAT)-equivalent features only. As a result, the engineering rules for this setup mimic those required for MAT.

Software limits

Hard-coded limits

The following section lists the hard-coded limits in the OTM software.

Table A-1 outlines the maximum value for many of the parameters associated with the various components of OTM.

Table A-1 OTM capacity parameters

Parameter	Maximum Value
Windows Common Services	
Maximum number of Sites that can be created on an OTM server.	3000
Maximum number of Branch Office systems can be created under a specific site	256
Maximum numbers of M1 synchronization / Update tasks (number of Log Windows) can be executed at the same time.	5
Number of Customers of M1 System.	100
Range of DN	0-99999999
Maximum numbers of Survivable Expansion Cabinet.	4
Maximum numbers of modem scripts can be created.	3000

Table A-1 OTM capacity parameters (*continued*)

Parameter	Maximum Value
Windows Common Services	
Maximum numbers of application jobs can be scheduled in the Scheduler application.	2000
Max String Length for:	
Site name	31
System name	31
Address	44
City	24
State/Province	24
Country	24
Zip/Postal Code	16
Comments	255
IP Address	15
Display (CPP profile)	1000
Timeout (CPP)	60
Phone Number (CPP)	50
Access ID (CPP)	50
Modem Password (CPP)	50
Modem Installation String (CPP)	50
Issue	99
System ID	16
Maximum Speed Call Lists	8191
Maximum ACD Agents	1200
PDT password	16
Customer Name	31
Directory Numbers	24
Customer Password	16
HLOC	9999
Dial Intercom Group	2045
User ID	2045

Table A-1 OTM capacity parameters (*continued*)

Parameter	Maximum Value
LDAP	
Maximum number of LDAP Sync Log files that can be created separately	2000
Number of LDAP entries that can be synchronized at the same time.	10,000
Number of entry can be added from LDAP Server to OTM Directory	15,000
Corporate Directory	
Maximum numbers of Customized Reports can be created.	2000
Number of Data fields can be defined into a corporate report	111
Maximum numbers of reports can be generated at the same time.	1
Maximum string length of all parameters.	255 characters
Data Buffering and Access (DBA)	
Maximum numbers of Action records can be defined in a DBA session.	1000
Maximum numbers of Rule records can be defined in a DBA session.	1000
Maximum numbers of CDR can be collected	5,000,000
List Manager	
Maximum numbers of speed call lists that can be created.	8190
Maximum numbers of group call lists that can be created.	63
Maximum numbers of group hunt lists that can be created.	8190
Maximum String length for:	
Speed Call List	
List Name	50
Entry Name	50
Dialed Digits	31
Speed Call List	
Entry Number	999
PLDN	31
Group Call list:	
List Name	50
Entry Name	50
Entry Number	19
Group Hunt List:	
List Name	50

Table A-1 OTM capacity parameters (*continued*)

Parameter	Maximum Value
Maximum String length for:	
Group Hunt List:	
PLDN	50
Dialed Digits	31
Entry Name	50
Entry Number	95
Station Administration	
Maximum number of External Parties that can be created	5000
Maximum number of Role/Projects that can be created	5000
Maximum number of employees that can be created	16,000
Maximum string length of all parameters.	128 characters
OTM DECT	
Maximum number of DECT Systems	500
Maximum String length for:	
DECT system name	255
Password	Unlimited
IP Address	15
OTM server IP Interface	15
Phone Number	64
PARI (Access Right Identification tab)	8
SARI (Access Right Identification tab)	8
Upstream Manager IP address (Access Right Identification tab)	15
Maintenance Windows	
Maximum number of maintenance commands that can be run at the same time	10
Maximum numbers of maintenance commands that can be executed at the same time in Web Maintenance	10
OTM Web	
Maximum number of clients that can log on to the Administration page of the same OTM server at the same time.	5

Table A-1 OTM capacity parameters (*continued*)

Parameter	Maximum Value
OTM Web	
Maximum number of clients that can log on to the web EndUser page of the same OTM server at the same time	20
Maximum number of sessions that can be controlled by OTM web server	1000
Maximum number of telephones that can be assigned to an end user	200
Data Buffering and Access (DBA)	
Maximum number of Meridian 1 or Succession CSE 1000 systems	256
Corporate database	
Maximum number of organizational levels	20
Virtual Terminals	
Maximum number of Virtual Terminals that can be enabled at one time	256
Call Detail Recording (CDR)	
Maximum number of call records per costing configuration in TBS	2,500,000
Maximum number of call records for CCCR	5,000,000
Alarm Management	
Maximum number of traps in the circular queue	1360 (see Note)



Note: A single Meridian 1 produces alarms, on average, at the rate of one every 10 seconds. This means the queue can hold 3.7 hours worth of alarms from a single Meridian 1 system without losing alarm information. Starting with Release 25 of Meridian 1 system software and in all releases of Succession CSE 1000 system software, there is the capability of filtering traps, on the PBX, based upon their categorization (for example, minor, major, critical, and so on). This can greatly reduce the alarm rate by permitting only major and critical alarms to be sent to OTM. Filtering increases the number of Meridian 1 and Succession CSE 1000 systems that can be connected. However, when a single Meridian 1 or Succession CSE 1000 system begins having a problem, it begins reporting major/critical alarms at the rate of 1 every 2 seconds. This means that the queue can hold only the last 45-minutes worth of alarms from the offending system, assuming that alarms from the other systems are minimal.

Operational limits

OTM Web interface

Usage of the OTM Web interface has the advantages of not requiring installation of the OTM Client and providing the ability to access the OTM Server from any PC with a Web browser. However, using the Web interface places a heavier workload on the OTM Server. The Web Desktop Services Write capability was introduced in OTM 1.1, and provides end users as well as administrators with the ability to configure telephones using a Web interface. After a telephone's configuration has been changed and scheduled, the job is placed into the queue of the scheduler.

The scheduler executes the jobs in the queue one by one. This impacts the throughput of the system. There is a delay between the time that the job is scheduled and the time that the job is finished. While the job is being executed, the peak CPU usage may approach 100 percent causing a performance degradation to other applications.

Web Station

Web Station Write capability requires more OTM Server resources than earlier versions of OTM without this capability. For example, a station change performed through the Web interface takes up to 48 seconds of CPU time (2 seconds for finding, 24 seconds for changing, and 22 seconds for transmitting), while a change through the Windows Station Administration application requires only 23.8 seconds of CPU time (1 second for finding, 0.8 seconds for changing, and 22 second for transmitting). If you schedule a job to run during off-hours, then the total CPU time is only 1.8 seconds for a change using the Windows Station Administration application.

Performance of station administration activities primarily through the Web interface using the Schedule Now function places a larger workload on the OTM Server. For example, in a system with 10,800 lines and a daily change rate of 1 percent, Add/Move/Change activity through the Web interface consumes up to 36.0 percent of CPU usage compared to only 23.8 percent if performed using the Windows interface.

Web Desktop Services for end users

When you configure the write capability for end users in Web Desktop Services, you place a higher workload on the OTM Server. For example, in a system with 10,800 lines and an end user daily change rate of 0.25 percent (approximately 27 telephones), enabling the write capability for end users in Web Desktop Services increases CPU usage for Add/Move/Change activity from 23.8 percent to 29.8 percent. Note that the ability for end users to make changes may decrease the need for the network administrator to make changes; therefore, the impact of configuring the write capability for end users in Web Desktop Services may not be significant in certain configurations.

Web support on Server and Workstation platforms

Table A-2 outlines the differences observed in Web support when OTM is running on server grade platforms and workstation platforms. Additional differences between the Windows NT Server and Windows NT Workstation platforms are given in Table A-4 on page A-17.

Table A-2 Web support on Servers and Workstations

	IIS on Windows NT Server or Windows 2000 Server	PWS on Windows NT Workstation or Windows 2000 Professional
Concurrent Internet Explorer sessions	Only limited by OTM capacity	5
Concurrent Netscape Navigator sessions	Only limited by OTM capacity	2
Restricted Access by IP address and domain name	Yes	No

Personal Web Server (PWS) is only intended to provide low-volume Web publishing capability. Performance degrades with increased traffic and complex Web pages or Java applications. The number of sessions supported by PWS is based on a ten-connection limit. Internet Explorer uses two connections per session, while Netscape Navigator uses between four and six connections depending on the size of the Web page.

When additional clients attempt to access Web Services and there are no available connections, an error message appears (Figure A-1).

Figure A-1 Too many users are connected error message

Modems

A modem connection between the OTM Client and the OTM Server is used for the command line interface (CLI) and Web applications. The OTM Server can operate as a terminal server, and the OTM Client uses the CLI to access the Meridian 1 or Succession CSE 1000 system. Nortel Networks recommends that you migrate to Web applications and access OTM features in a Client/Server configuration using a modem connection.

Operational testing

The test setup was:

- A 450 MHz Pentium II with 256 MB of memory and ATAPI hard disk interface
- A Meridian 1 Option 61C/81C, and assumes that 1% of a total of 1000 lines are changed on a daily basis by the network administrator

For an Option 11C or Succession CSE 1000 system, decrease CPU usage by a factor of 2 and increase elapsed time by the same factor for those features that interact with the system (for example, Station Update, but not Cost Report).

- A 100 MB network

Table A-3 lists those OTM applications that have a significant impact on the performance of the OTM Server PC. The table lists CPU utilization and elapsed time statistics, as appropriate, when connected to a single Meridian 1 or Succession CSE 1000 system.

Table A-3 PC performance by application

Application	Real Time (CPU)		Elapsed Time
	Peak	Average	
Station Administration Add/Chg/Del		2.2%	
Station Reconcile with Meridian 1 system	100%		1 record/3 seconds
Web Station Administration	100%		1 record/48 seconds
Web Desktop Services write capability for end users	100%		1 record/48 seconds
Web Admin		Negligible	
Alarm Monitor	2%	Negligible	
DBA - CDR Collection	6%	3%	
DBA - Traffic Collection	1%	0.5%	
LDAP Sync*	100%		10 records/second
Parsing CDR File	100%		40 records/second
Cost Report	100%		40 records/second
OTM Client (Station Update)	4%		1 record/5 seconds

- * LDAP Sync testing was based upon the use of an LDAP server dedicated for this testing. Since OTM does not control the LDAP Server used in the customer network, the server response time is likely to be less. Factors for the LDAP Server, such as processor speed, other uses for LDAP Server (for example, Corporate Directory), other LDAP clients, and other services running on the same platform impact this server's resources.

PC hardware

This section describes the PC hardware requirements necessary to run OTM optimally. Start with the "OTM Server hardware requirements" on page A-12. Also, follow these guidelines using the information provided in the sections "Physical memory" on page A-14, "Hard disk" on page A-15, and "Processor speed" on page A-17:

- Add additional serial interface cards as needed.

- Calculate disk storage requirements based on applications usage.
- Implement a backup and restore strategy.
- Follow regular maintenance instructions as documented for OTM features to maintain the integrity and capacity of the hard disk.
- Add disk redundancy as required.
- Increase performance by:
 - Adding more system memory
 - Utilizing a faster hard disk or SCSI interface, or both
 - Using a faster CPU
- Scale your PC for future growth, and utilize a PC that:
 - Has a reserve PCI Card slot for a SCSI Interface Card (See “Hard disk” on page A-15 for details.)
 - Has a spare storage bay and power for adding an internal hard disk
 - Can accommodate increasing the memory capacity to 1GB or greater (Most PCs have 2 to 4 memory card slots that can accommodate 64 MB, 128 MB, 256 MB, and so on, DIMMS.)



Note: Response time testing is based upon the recommended configuration, not the minimum configuration. Response time performance is only supported on the recommended configuration.

OTM Server hardware requirements

The OTM Server must meet the following hardware requirements.

- 400 MHz Intel Pentium II Processor or equivalent minimum; 600 MHz Intel Pentium III processor recommended
- 2 GB hard drive or greater (1000 MB free space plus customer data storage requirements) with ATAPI interface (Refer to “Hard disk” on page A-15 for details.)
- 256 MB of RAM minimum; 512 MB of RAM recommended (Refer to “Physical memory” on page A-14 for details.)
- CD-ROM Drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA color monitor and interface card using a minimum monitor setting of 800 by 600

- Two Ethernet Network Interface cards to support connection with the Meridian 1 or Succession CSE 1000 system via Ethernet and Customer LAN
- Optional Hayes-compatible modem for connection to remote systems, required for polling configurations (56 K BPS)



Note: OTM does not support software-based modems.

- Dongle (for server or stand-alone only)
- Printer port (LPT) required for dongle
- PC COM port with 16550 UART
- Windows-compatible mouse or positioning device (PS2 mouse preferred to free up a PC serial port)



Note: Do not install OTM on a Microsoft Windows NT or Windows 2000 system that is configured as a primary domain controller (PDC).

Single (stand-alone) OTM hardware requirements

OTM running in stand-alone mode requires the following:



Note: Stand-alone mode consists of a single web-based Client and no Windows Clients.

- 233 MHz Intel Pentium II processor or equivalent minimum; 400 MHz Intel Pentium III processor or higher is recommended
- 2 GB hard drive with 500 MB of free space with IDE interface
- 128 MB of RAM (256 MB of RAM is recommended for improved performance and for the Billing Enhanced level applications.)
- CD-ROM drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA color monitor and interface card using a minimum monitor setting of 800 by 600
- Ethernet network interface
- Dongle (for server or stand-alone only)

- Printer port (LPT) required for dongle
- Windows-compatible mouse or positioning device
- Windows 98, Windows 2000, or Windows NT Workstation 4.0 or Server

OTM Windows Client hardware requirements

An OTM Client (a computer that accesses the OTM Server) requires the following:

- 233 MHz Intel Pentium II processor or equivalent; 400 MHz Pentium III or higher is recommended
- 2 GB hard drive with 500 MB of free space with IDE interface
- 128 MB of RAM minimum; 256 MB of RAM is recommended
- CD-ROM drive and 3 1/2-inch, 1.44 MB floppy disk drive
- SVGA color monitor and interface card using a minimum monitor setting of 800 by 600
- Ethernet network interface
- Windows-compatible mouse or positioning device
- Windows 98, Windows 2000 Professional, or Windows NT Workstation 4.0

OTM Web Client hardware requirements

A Web Client (a computer that uses a web browser to access the OTM Server) requires the following:

- Equipment capable of running IE 5.0, 5.5, 6.0, or Netscape 4.7.

Physical memory

The amount of physical memory installed on the server is critical in achieving maximum performance on the PC. Microsoft Windows systems have a feature called Virtual Memory. Virtual Memory allows the PC to continue running programs that require more memory than there is physical memory available. It borrows memory using a memory-swapping scheme from available space on the

main hard disk. Although this feature permits the PC to perform operations without worrying about running out of physical memory and, thus, crashing the computer, it sacrifices performance of these operations by requiring access of the hard disk while memory swapping. This degrades performance because:

- Physical memory access is much faster than disk access.
- Accessing the disk while memory swapping steals disk resources away from applications that need to read and write to the hard disk.

The OTM Server software and the Windows NT Server software require ~150 MB without active features. The minimum server memory is 256 MB.

The amount of memory does not grow significantly as features are running and windows are opened.

The one exception to this is OTM Client access. Each OTM Client connection to the OTM Server requires an additional 3 MB of memory. For large configurations, such as 100 Meridian 1 systems and 50 OTM Clients, an additional 150 MB of memory is required.

Hard disk

Disk performance

Much of the time spent by OTM Features is in reading and writing data to the hard disk. Features that spend a good percentage of their time accessing the disk are called disk-intensive applications. For these features, the access time is critical in terms of the time it takes for a feature to complete an operation.

OTM disk-intensive applications analyzed in this document include:

- CDR and traffic collection
- TBS report generation
- Simultaneous Meridian 1 Update of Station Data

Station Update from a single Meridian 1 is not affected by disk performance, as the speed of transmission from the Meridian 1 is slower than the PC accessing its disk.

- Web/OTM Client Station Access

“OTM Server hardware requirements” (page A-12) recommends a hard disk using the ATAPI interface. It also recommends a single hard disk.

Performance improvements can be achieved by:

- Using the fastest Ultra-Wide SCSI Interface (15K RPM)
Disk Performance increases by a factor of 2 or better. This can translate to an increase in feature performance (reduce elapsed time and increase simultaneous operations) by 50 percent or better.



Note: SCSI disk drives come in various speeds.

- Adding a hard disk to store OTM Data separate from the OS and Programs
If the Server PC being used is using an ATAPI interface for its main disk, C:, then installing a SCSI interface card and second hard disk to store OTM Data can achieve the majority of the SCSI performance increase.

Disk size

The OTM Server software and the Windows NT Server software requires approximately 900 MB without OTM data or active features.

You must reserve approximately 300 MB of disk space for virtual memory and normal OS operations.

CDR = 250 bytes per record, at peak rates (for a CP4-Option 81 system) over a one-day period, this creates a 700 MB file.

Station~ = 500 kb per 100 telephones. From the example in Tables A-8 and A-7:
Disk space = 500 kb/100 telephones * 10,000 lines = 50 MB of disk space.

Directory~ = 80 kb per 100 records. From the example in Tables A-8 and A-7:
Disk space = 80 KB/100 telephones * 10,000 lines = 8 MB of disk space.

Processor speed

The 600 MHZ CPU recommended is sufficient for the maximum configurations presented here.

An increase in CPU power does not, by itself, greatly increase the capacity of the Server.

The PC is so I/O bound, from accessing memory to accessing the hard disk, that a two-fold increase in CPU power may result in only a 10 percent increase in OTM capacity.

Replacement of the motherboard, not just the CPU chip, can further increase CPU performance, since the newer motherboard is designed to take advantage of the high processor speeds (for example, faster CPU bus, faster memory, and so on). The PC is still heavily bound to disk access and network speeds.

Windows NT Server and Windows NT Workstation differences

Table A-4 shows the differences between Windows NT Workstation and Windows NT Server.

Table A-4 Differences between Windows NT Server and Windows NT Workstation

	Windows NT Server	Windows NT Workstation
Purpose	Network Server	Multitasking Desktop OS
CPU	Up to 4	Up to 2
Incoming concurrent session	Unlimited (limited only by number of licenses possessed)	10
Remote Access Service	Up to 256 simultaneous sessions	1
Directory Replication	Import and Export	Import
Disk Fault Tolerance	Yes	No
Logon Validation	Yes	No

Table A-4 Differences between Windows NT Server and Windows NT Workstation (*continued*)

	Windows NT Server	Windows NT Workstation
Service for Macintosh	Yes	No
Internet Service	Internet Information Server (IIS)	Personal Web Server (PWS). PWS does not have the feature to restrict access by IP address.

Network bandwidth

Typical configurations

Figure A-2 shows how OTM connects to Meridian Mail and to older Meridian 1 systems that are not packaged with Ethernet. In this scenario, OTM is connected to these systems through their serial ports. Physical limitations on serial connections limit OTM to be placed within 15.24 meters (50 feet) of these systems to minimize noise, which can cause transmission errors.

OTM Clients can dial up to the OTM Server and use CLI to access the Meridian 1 systems. For full access to OTM features, the OTM Client can also use OTM's Web interface. An OTM user can connect to OTM using a remote access software package (for example, pcANYWHERE*).

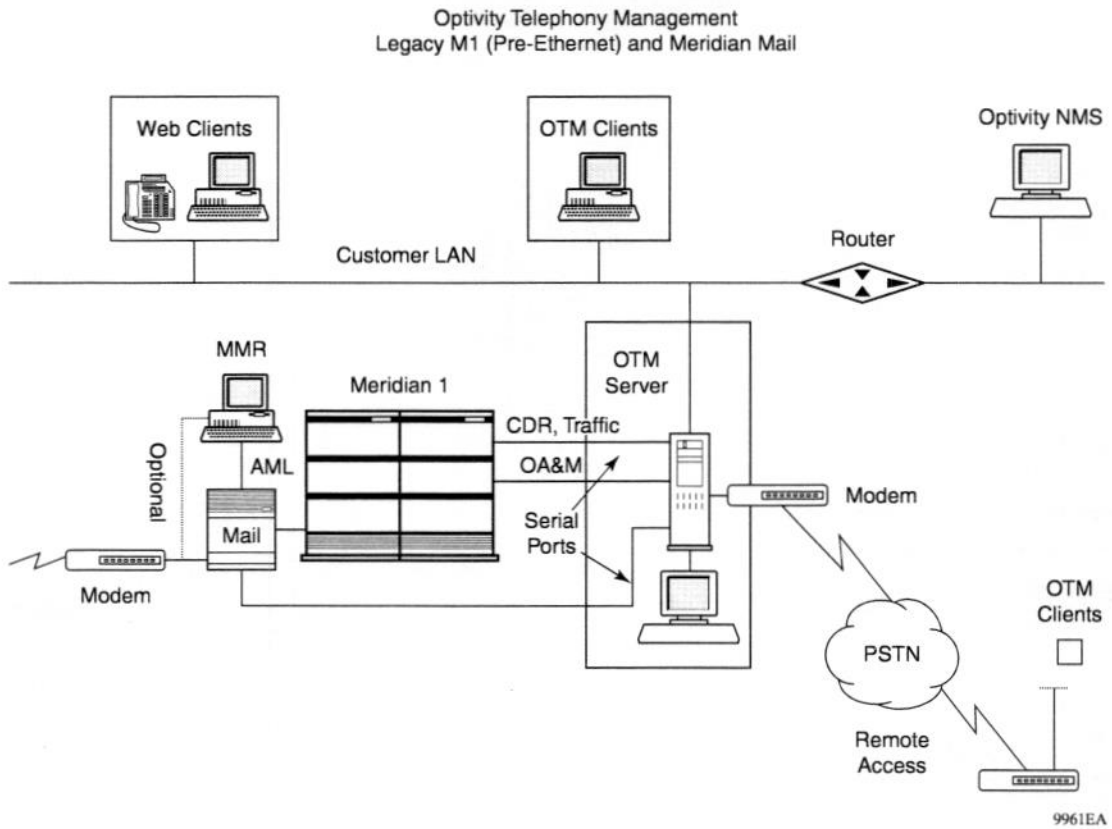
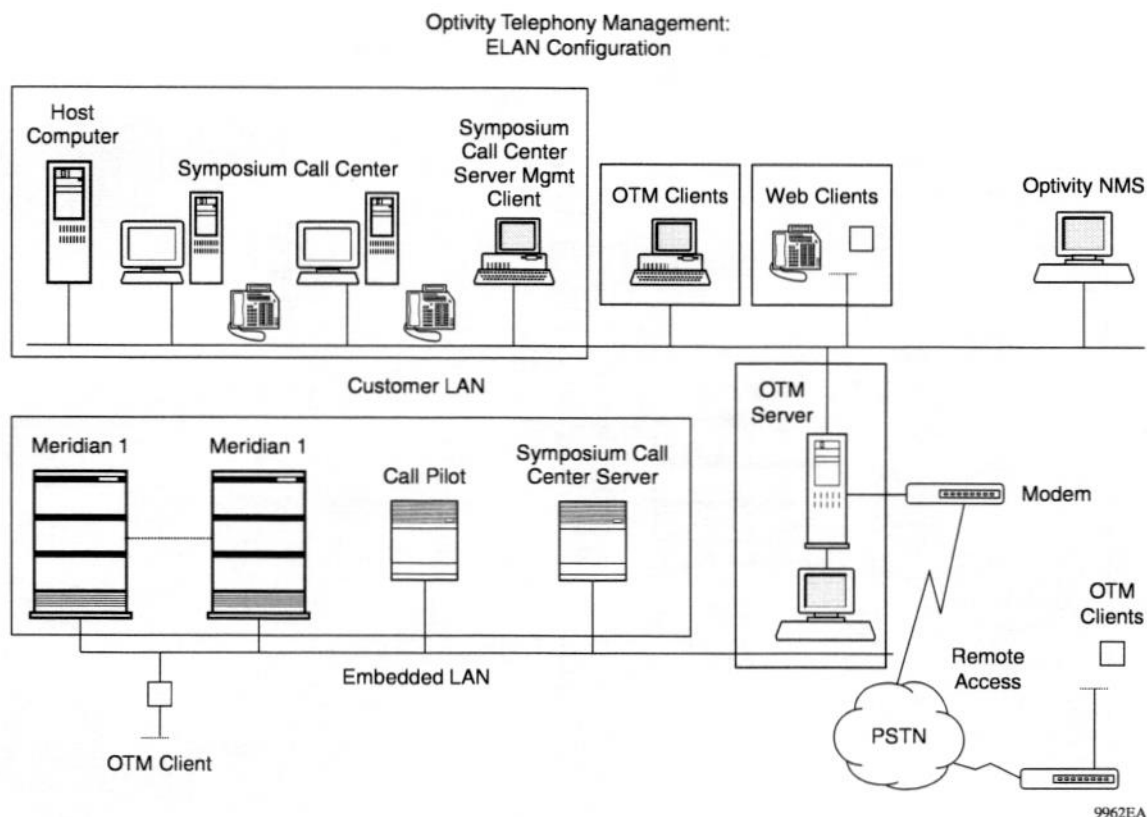
Figure A-2 Connecting OTM to legacy Meridian 1 systems (pre-Ethernet)

Figure A-3 represents how OTM connects to Meridian Applications and to Meridian 1 and Succession CSE 1000 systems that are packaged with Ethernet. In this picture, OTM is connected to these systems via Ethernet using the Meridian 1 or Succession CSE 1000 system's embedded LAN (ELAN). Meridian 1 and Succession CSE 1000 systems require that the ELAN be protected from the customer's LAN. Therefore, if OTM is to be connected to the customer's LAN (CLAN), to provide Client Access to the OTM Server, then OTM must have two Ethernet cards, one for connecting to the ELAN and one for connecting to the CLAN.

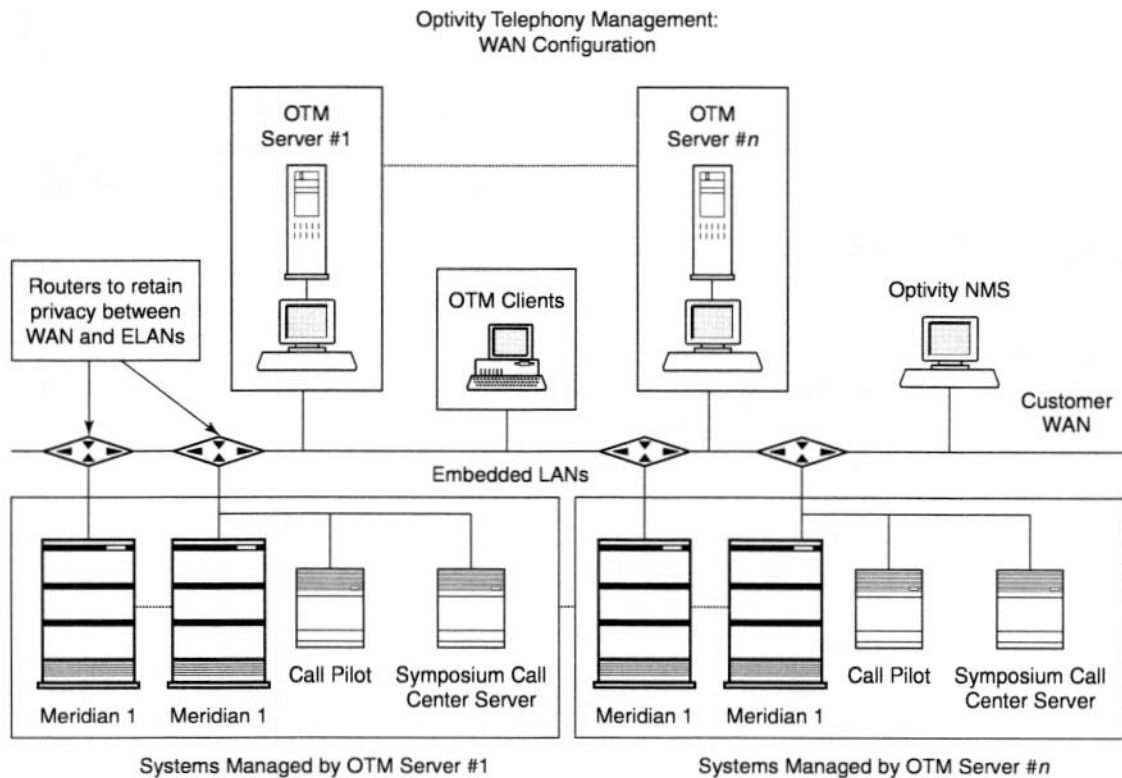
Figure A-3 Connecting OTM to ELAN connected Meridian 1 and Succession CSE 1000 Systems

This configuration provides optimum performance, as all communications between OTM and the Meridian 1 or Succession CSE 1000 systems are private. In this case, there is no impact to this communication due to Customer LAN traffic. It also meets the requirement of protecting the ELAN from the CLAN as required for Meridian 1 and Succession CSE 1000 systems by having OTM act as a router.

Physical limitations on 10 Mbps Ethernet connections limit the ELAN distance to 500 meters (1640 feet) using a maximum of four hubs/repeaters. The maximum distance from end device to hub and hub-to-hub is 100 meters (328 feet). Creation of a separate embedded WAN (EWAN), which connects ELAN segments utilizing switches or routers, or both, can be used to increase distance. These switches/routers must be used for only this EWAN. The additional cost of an EWAN network configuration, as well as the additional wiring necessary to connect a geographically disperse environment (one that spans multiple floors or buildings, or both), can make the EWAN option less practical.

Figure A-4 pictures OTM connected directly to the customer WAN (CWAN). Connection of the ELAN to the CWAN via routers provides protection for the ELAN segments. This configuration solves the problem of connecting a single OTM Server to multiple Meridian 1 and Succession CSE 1000 systems, when these systems are geographically disperse, without requiring a separate network. It also permits OTM to be connected to a larger number of systems from a traffic perspective, for Customer WANs that are utilizing higher bandwidths (for example, 100 Mbps, 1 Gbps, and so on). The disadvantage is that available bandwidth must be shared with Customer traffic.

Figure A-4 Connecting OTM to CWAN connected Meridian systems



9963EA

Bandwidth utilization

The trade-off is the cost of OTM versus the cost of increased network bandwidth or network subnets, or both. Once OTM Servers are attached to the WAN, the customer's network may be impacted, but there is a saving on the number of OTMs needed.



Note: Never expect to fully utilize Ethernet bandwidth. Performance degrades quickly as the utilization exceeds a certain threshold (approximately 35 percent). Consult the network administrator for details on network bandwidth utilization.

Table A-5 lists the average and peak traffic for the ELAN and CLAN. This is based upon traffic analysis of a Meridian 1 running on a CP4 CPU. For an Option 11C or Succession CSE 1000 system, divide the ELAN numbers by 2, except for alarms. For the CPP CPU, multiply the ELAN numbers by 4, except for alarms.

Table A-5 Network bandwidth usage per Meridian 1 system

OTM Activity	Transfer rate (bits/second)	
	Average	Peak
Station Add/Chg/Del, ELAN	32 kb	32 kb
Station Sync with M1, ELAN	NA	48 kb
CDR, ELAN	35 kb	70 kb
Traffic, ELAN	24 kb	48 kb
Alarm, ELAN	1 kb	3 kb
Sync with LDAP Server, CLAN	NA	720 kb
Total, ELAN	~92 kb	~201 kb
Total, CLAN		~720 kb

Alarm Processing

OTM alarm details

The OTM Trap Server can handle 25–50 incoming SNMP traps per second. However, this limitation varies considerably with network load, PC processing power, and CPU availability.

Traps are stored in a circular queue of 1360 traps. You can view the queue using the Web Alarm Browser. If the rate of trap arrival is heavy, some traps are not entered into the queue even though they are received by the Trap Server and Alarm Notification application. The circular queue can handle an incoming rate of 50 traps in 10 seconds without any loss of information.

An SNMP trap has an average size of approximately 400 bytes. You can use this information to approximate the bandwidth requirements for trap processing. For example, 1000 devices, each producing one trap every 10 seconds, would require a bandwidth of 320 Kbps.

$400 \text{ bytes/trap} * 8 \text{ bits/byte} * 1000 \text{ devices} * 0.1 \text{ trap/sec/device} = 320 \text{ Kbps}$

ITG/Switch alarm details

Under normal conditions, a Meridian 1 system generates one trap approximately every ten seconds. Beginning with X11 Release 25, you can use filtering on the Meridian 1 to reduce the output of traps. However, there is no filtering capability on ITG. ITG does not generate traps under normal operating conditions. In an abnormal situation, ITG could be expected to generate an alarm every 5 seconds.

ITG may generate a large number of alarms when Quality of Service (QoS) monitoring is enabled. When QoS monitoring is enabled, an alarm is raised or cleared for every QoS threshold crossing (excellent, good, or fair) per codec. A network with varying QoS will have many threshold crossings resulting in a large number of alarms.

Recommended usage

For bandwidth and processing reasons, alarm traffic should be minimized. If alarms from the switch are sent to OTM, use filtering to limit the traffic to only important alarms. Since it is unlikely that multiple ITG cards will simultaneously exhibit problems, the alarms generated by ITG cards should not create traffic problems. To limit alarm traffic, Nortel Networks recommends that you not enable Network QoS Monitoring. Changes to ITG to allow filtering will help this situation. The incoming rate of alarms must match the handling capabilities of the OTM configuration.

The alarm circular queue can be quickly exhausted if there is significant alarm traffic.

ITG operational measurement processing

Operational measurement details

ITG cards collect operational measurement (OM) information on an hourly basis. This data is stored on the cards until it is retrieved by OTM using an FTP operation. The data can be retrieved on demand, however, the FTP operation is normally scheduled to occur on a daily basis. The data file generated by an ITG card in a 24 hour period is approximately 5 KB.

When retrieval occurs, the information is collected from all cards on all nodes. There is no capability to retrieve the information on an individual node basis.

The retrieved information is parsed and written to comma separated values (CSV) files on the OTM Server. The number of files created is dependent upon the number of records retrieved.

Recommended usage

If there are a large number of cards in the system, the retrieval operation should be scheduled to occur during off-hours.

OTM System Performance

Network impact on OTM Windows Client/Server

Network performance has a significant impact on OTM Windows Client/Server applications.

Figure A-5 shows the relationship between Station Administration response time and RTT (Round Trip Time) in a lab environment. Customers may experience different response times depending on their network performance.

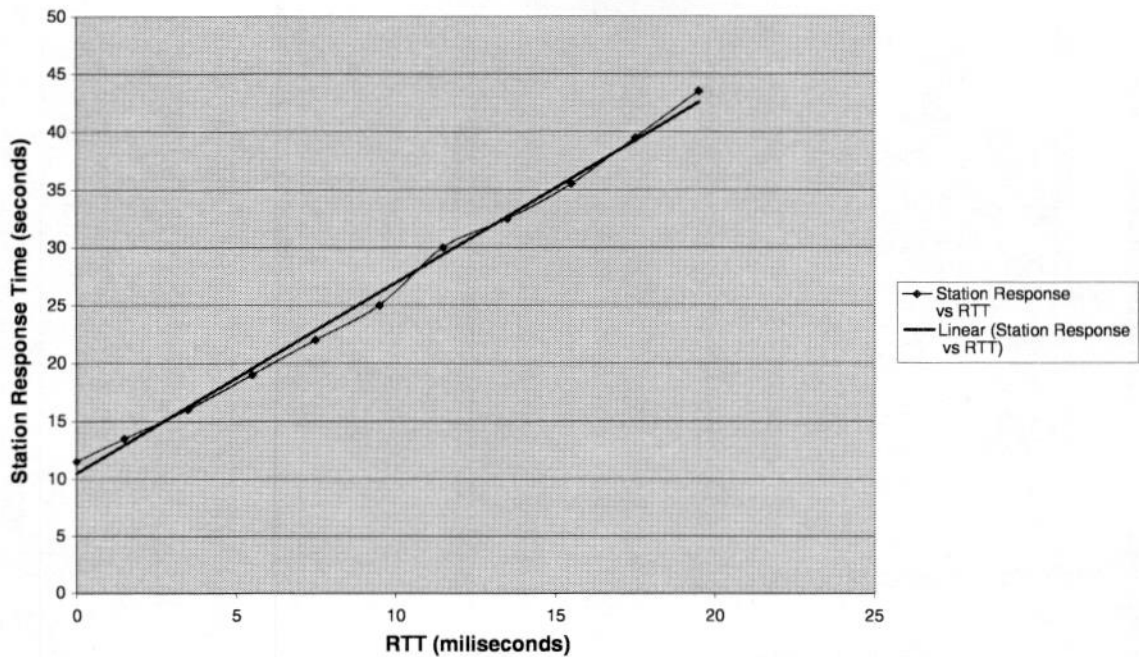
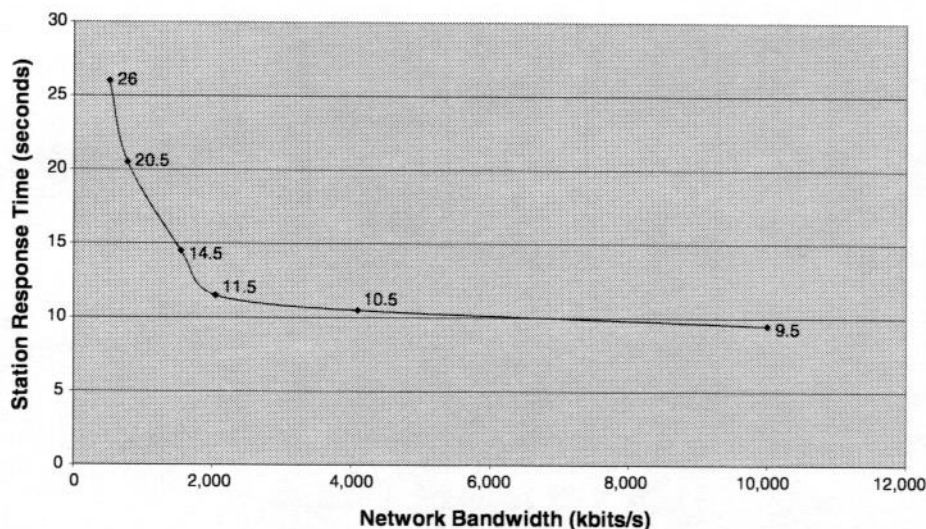
Figure A-5 Station Administration Response Time versus Round Trip Time

Figure A-6 shows the relationship between Station Administration response time and Bandwidth in a lab environment. Customers may experience different response times depending on their network performance. Note the negative exponential impact of using bandwidth that is less than 2 Mbps.

Figure A-6 Station Administration Response Time versus Network Bandwidth

Hostname resolution

LMHOSTS file

When Microsoft TCP/IP is used on a local network with any combination of computers running Windows 98, Windows NT, Windows 2000, and so on, server names are automatically matched to their corresponding IP addresses. However, to match server names across remote networks connected by routers (or gateways), the LMHOSTS file can be used if WINS servers are not available on the network. Figure A-7 and Figure A-8 show an example of an LMHOSTS file.

The LMHOSTS file is commonly used to locate remote computers for Microsoft networking file, printer, and remote access services, and for domain services such as logon, browsing, replication, and so on.

Microsoft TCP/IP loads the LMHOSTS file into memory when the computer is started. The LMHOSTS file is a text file in the Windows directory that lists the IP addresses and computer names of remote Windows networking servers that you want to communicate with. The LMHOSTS file should list all the names and IP addresses of the servers you regularly access.

For example, the LMHOSTS table file entry for a computer with an address of 192.53.63.2 and a NetBIOS computer name of Building1 would be:

192.53.63.2 Building1

To create an LMHOSTS file:

- 1 Use a text editor to create a file named LMHOSTS.

Or

Edit the default file named LMHOSTS.SAM.

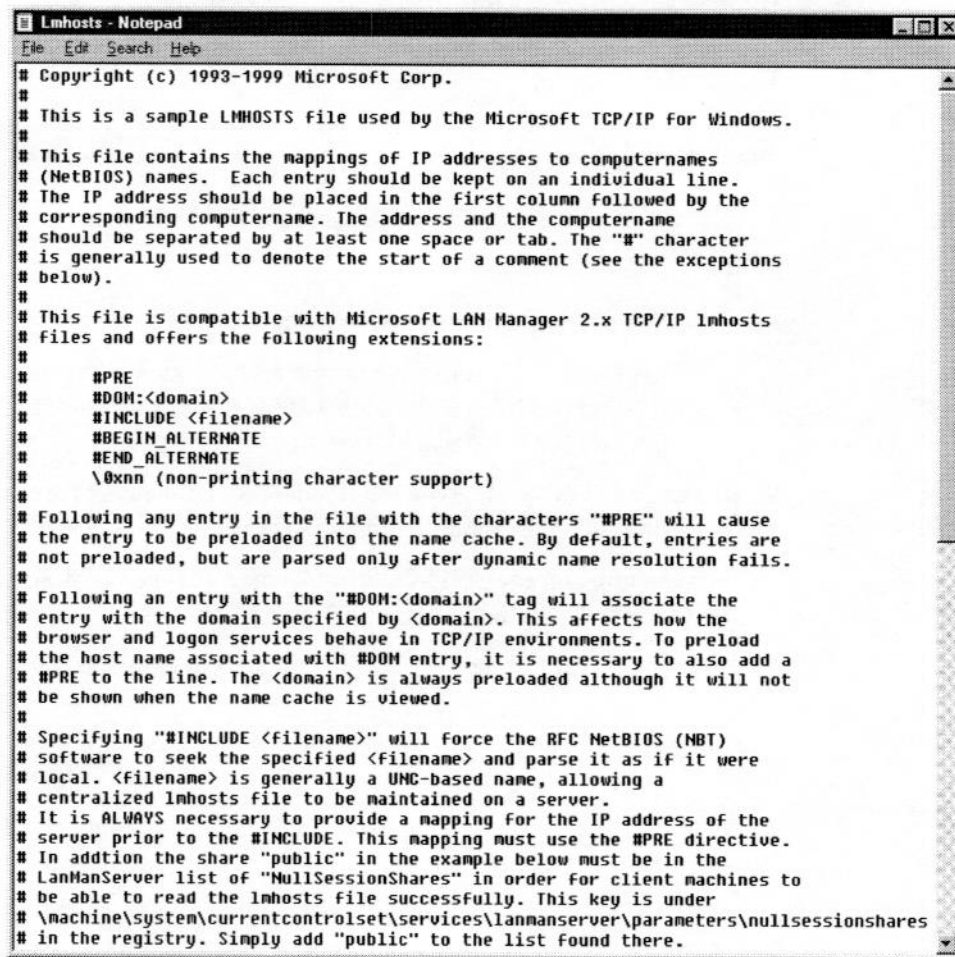
This file is located in the **<system root>**\system 32\drivers\etc directory for Windows NT and Windows 2000 systems and in the C:\Windows directory for Windows 98 systems.

- 2 In the LMHOSTS file, type the IP address and the host name of each computer that you want to communicate with.

For example, on each OTM Client machine add the OTM Server name and its IP address. Separate the items with at least one space.

Note that entries in the LMHOSTS file are not case-sensitive.

Figure A-7 Example of LMHOSTS file (part 1)



```

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names. Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lnhosts
# files and offers the following extensions:
#
#       #PRE
#       #DOM:<domain>
#       #INCLUDE <filename>
#       #BEGIN_ALTERNATE
#       #END_ALTERNATE
#       \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
# In addition the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
# \machine\system\currentcontrolset\services\lanmanserver\parameters\nullsessionshares
# in the registry. Simply add "public" to the list found there.

```

Figure A-8 Example of LMHOSTS file (part2)

```

# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE
# statements to be grouped together. Any single successful include
# will cause the group to succeed.
#
# Finally, non-printing characters can be embedded in mappings by
# first surrounding the NetBIOS name in quotations, then using the
# \0xnn notation to specify a hex value for a non-printing character.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97      rhino          #PRE #DOM:networking  #net group's DC
# 102.54.94.102     "appname \0x14" #special app server
# 102.54.94.123     popular        #PRE                #source server
# 102.54.94.117     localsrv       #PRE                #needed for the include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
# character in its name, the "popular" and "localsrv" server names are
# preloaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.

102.54.94.123      otmservr1       #PRE                #OTH server

```

3 Save the file as LMHOSTS.

Note that the filename is LMHOSTS with no extension.

LMHOSTS is normally used for smaller networks, or to find hosts on remote networks that are not part of the WINS database (because name query requests are not broadcast beyond the local subnetwork). If WINS servers are in place on an internetwork, users do not have to rely on broadcast queries for name resolution, because WINS is the preferred method for name resolution. Therefore, with WINS servers in place, LMHOSTS may not be necessary.

The LMHOSTS file is read when WINS or broadcast name resolution fails. Resolved entries are stored in a system cache for later access. When the computer uses the replicator service, and does not use WINS, LMHOSTS entries are required on import and export servers for any computers on different subnetworks participating in the replication.

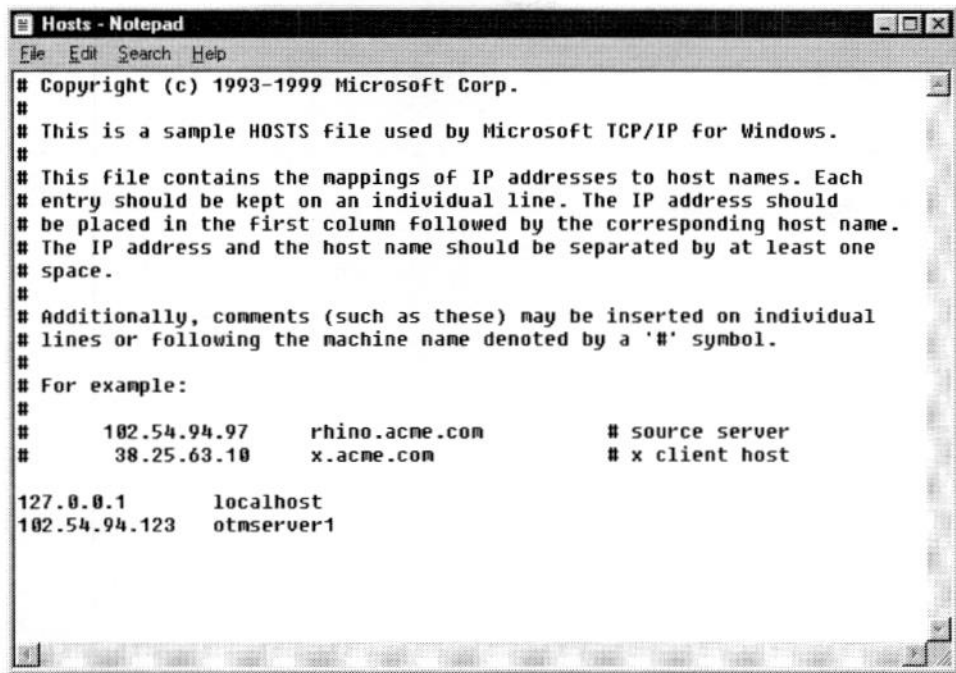
To configure TCP/IP to use LMHOSTS on a Windows 2000 PC:

- 1** Open Network and Dial-up Connections.
- 2** Right click the network connection you want to configure, and then click Properties.
- 3** On the General tab (for local area connection) or the Networking tab (all other connection), click Internet Protocol (TCP/IP), and then click Properties. Click Advanced, click the WINS tab. Select the Enable LMHOSTS lookup check box. This option is enabled default.
- 4** To specify the location of the file that you want to import into the LMHOSTS file, click Import LMHOSTS, and then select the file in the Open dialog box.
- 5** To complete the configuration, either:
 - a** Reboot the computer
Or
 - b** Go to the command prompt, and enter the following text:

```
nbstat -R  
nbstat -c
```

HOSTS file

The HOSTS file contains a list of host name to IP address mappings. It is a regular text file. The HOSTS file is located in the **<system root>**\system 32\drivers\etc directory for Windows NT and Windows 2000 systems. For Windows 98 systems, the HOSTS file is located in the C:\Windows directory.

Figure A-9 Sample HOSTS file

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com      # source server
#       38.25.63.10     x.acme.com         # x client host

127.0.0.1      localhost
102.54.94.123  otmsvr1
```

Use a text editor to edit the HOSTS file. In the HOSTS file, type the IP address and the host name of each computer that you want to communicate with, for example, on each OTM client computer add the OTM Server IP address followed by its name. Separate the items with at least one space. Entries in the HOSTS file are not case-sensitive. Note that the HOSTS filename has no extension.

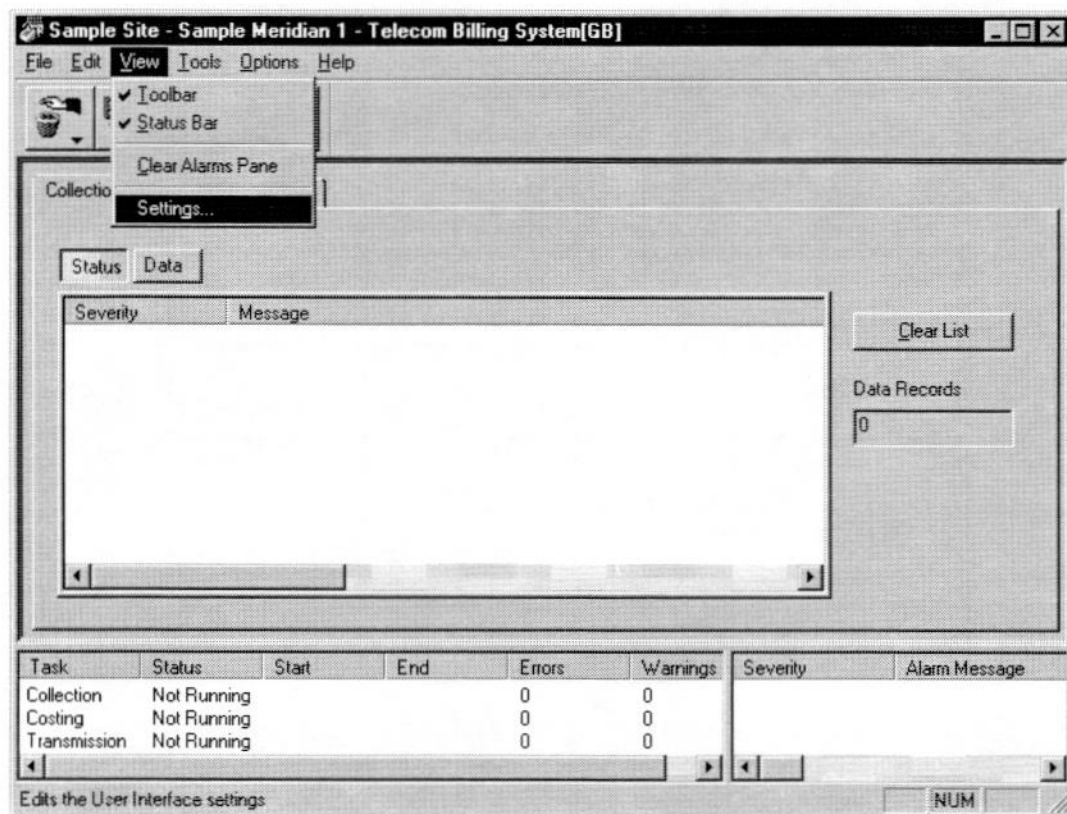
Telecom Billing System Display option

The Telecom Billing System (TBS) Display option for collecting, costing, and transmitting call records negatively impacts system performance by consuming system resources.

To improve system performance, disable the Display option:

- 1 In the Telecom Billing System application, select View > Settings (Figure A-10).

Figure A-10 Telecom Billing System



The Settings dialog box opens with the Collection tab selected (Figure A-11).

Figure A-11 Settings dialog box—Collection tab

- 2 Ensure that the Display CDR records as they are collected check box is unchecked.
- 3 Click the Costing tab.

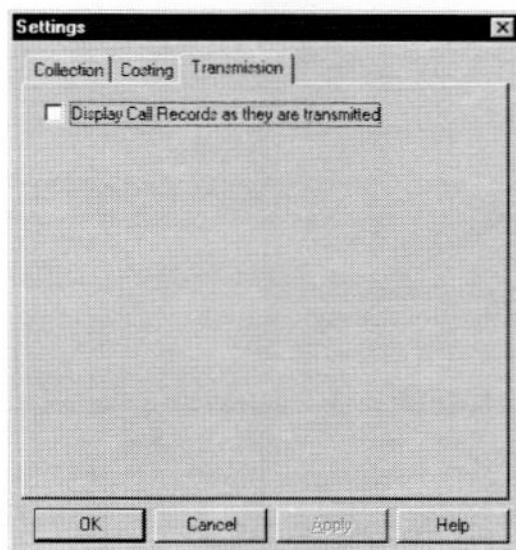
The Settings dialog box—Costing tab appears (Figure A-12).

Figure A-12 Settings dialog box—Costing tab

- 4 Ensure that the Display Call Records as they are costed check box is unchecked.
- 5 Click the Transmission tab.

The Settings dialog box—Transmission tab appears (Figure A-13).

Figure A-13 Settings dialog box—Transmission tab



- 6 Ensure that the Display Call Records as they are transmitted check box is unchecked.
- 7 Click OK.

OTM port usage

When using OTM to monitor and maintain systems, various ports and protocols are used to communicate between OTM and the desired client, server, or application. Table A-6 lists typical port usage based on the the flow of information between OTM and these system components.

Table A-6 OTM port usage

OTM Sending To:	Port	Type	Protocol	Component
Meridian 1 or Succession CSE 1000 system	513	TCP	Rlogin	Session Connect, System Terminal, Station Admin, CPND, List manager, ESN
Meridian 1 or Succession CSE 1000 system	161	UDP	SNMP	Alarm Management, Maintenance Window
Meridian 1 or Succession CSE 1000 system	21	TCP	FTP	Corporate Directory Upload
Meridian 1 or Succession CSE 1000 system	20	TCP	FTP	Corporate Directory Upload
Meridian 1 or Succession CSE 1000 system	1929	UDP		DBA Note: DBA uses 1 port per session, starting with port 1929.
SMTP server	25	TCP	SMTP	Alarm Notification
ITG	21	TCP	FTP	OTM ITG
WinClient	139	TCP	NetBEUI	Windows Client File Sharing
LDAP Server	389	TCP	LDAP	LDAP Synchronization
LDAP Server over SSL	636	TCP		LDAP Synchronization
OTM Receiving From:	Port	Type	Protocol	Component
Web Client	80	TCP	HTTP	Web CS, Desktop Services, Web Telecom Billing System
Web Client	4789–5045	TCP		Virtual System Terminal Note: VT uses 1 port per session, starting with port 4789.
Win Client	139	TCP	NetBEUI	Windows Client File Sharing
Win Client	3351	TCP	Btrieve	Station Administration Note: Station Administration uses 1 port per session, starting with port 3351.
Meridian 1 or Succession CSE 1000 Sending To:	Port	Type	Protocol	Component
OTM	162	UDP	SNMP	Alarm Traps (LD 117), Maintenance Window
OTM	1929	UDP		DBA Note: DBA uses 1 port per session, starting with port 1929.
DECT	5099	TCP	RMI	OTMDECT
Station	1583	TCP	Btrieve	Station Administration

Sample walk-through of computations

This section provides a sample walk-through of computations used to determine how many Meridian 1 or Succession CSE 1000 systems and OTM Clients can be connected to an OTM server. Factors involved include:

- Type of OTM feature configuration
- Type of OTM Server and Meridian 1 or Succession CSE 1000 hardware
- Constraints on CPU usage and off-hours work

Sample configurations based on application usage and features

The following are the sample configurations based upon application usage and features that impact server resources. These configurations do not reflect how OTM is packaged (for example, General, Enhanced, and Premium).

Example 1

Configuration

Station, ITG, Maintenance Windows, Alarm Management, MDECT configuration, and other applications

Example 2

Configuration and Alarm Management with Web/OTM Client Access and LDAP Service and Web Station Write configured for end users (full OTM system)

Example 3

Alarm Management, Data Buffering & Access (DBA), Traffic Analysis, OTM as a Buffer Box replacement (Access Server)

Sample PC and Meridian 1 configurations

The following are the PC and Meridian 1 configurations used for this example:

- OTM Server and OTM Clients connected to a 100 MB network, utilizing no more than 35 percent of its bandwidth



Note: Refer to Figure A-3 on page A-20.

- 512 MB of physical memory
- ATAPI Hard Disk
- 2 OTM Windows and/or Web Clients active at the same time at peak usage
- Option 11C averaging 400 lines per system
 - Averaging 1 call records/second generated (peak is 6)
- Option 81 with CP4 averaging 2000 lines per system
 - Averaging 3 call records/second generated (peak is 32)

Operational constraints

The following are the operational constraints:

- During normal operation do not use more than 80% of the CPU for routine operations to leave time to perform other operations. For example, Maintenance windows and ITG configuration.
Routine operations as defined in Table A-3 on page A-11 are:
 - Station Add/Move/Change from server
 - Station Add/Move/Change from OTM Client
 - Station Web access
 - Web Desktop Services Write capability for End Users
 - Alarms monitoring
 - CDR and Traffic Collection
- Normal operations are performed daily during normal working hours (for example, from 8:00 a.m. to 5:00 p.m. every day). The default value is the peak six hours of the day (9:00 a.m. to 12:00 p.m. and 1:00 p.m. to 4:00 p.m.).
Daily activities are based on the following assumptions:

- Percentage of lines changed by the network administrator per day is 1 percent. For example, a system with 2000 lines has 20 lines changes by the network administrator during a normal work day.
- Number of lines changed by end users through Web Desktop Services is 0.25 percent. For example, a system with 2000 lines has approximately 5 lines changed by end users during a normal work day provided that the Web Desktop Services Write feature is configured.
- Off-hours operations can use 100 percent of the CPU, and is limited as follows (from Table A-3):
 - Station retrieve/reconcile is performed once a week, or twice a month, on the weekend. The maximum period of time reserved for this activity is theoretically 48 hours. For these examples, reserve the time from 9:00 p.m. on Sunday to 6:00 a.m. on Monday, or 9 hours.
 - Station transmit will be scheduled and performed during the peak 6 hours (for example, from 9:00 a.m. to 12:00 p.m. and 1:00 p.m. to 4:00 p.m.).
 - Assume, for an Option 11C, that OTM can run Station update for two Meridian 1 or Succession CSE 1000 devices simultaneously (based upon processor speed and CPU usage figures).
 - CDR Reports are performed once a day. For these examples, off-hours are from 12:00 a.m. (midnight) to 6:00 a.m., or 6 hours.
 - LDAP Sync is performed once a week, on the weekend. For these examples, reserve the time from 9:00 p.m. Sunday to 6:00 a.m. on Monday, or 9 hours.

Table A-7 and Table A-8 provide OTM capacity estimates, based upon the information provided in the succeeding sections, and using the configuration examples previously defined. In the numbers presented, the most limiting factor from routine operation, off-hours operation, and network bandwidth is entered into the tables. The numbers in these tables were calculated as follows:

Table A-7 Maximum configuration for an Option 81 network averaging 2000 lines per system

Configuration example	Number of Meridian 1 systems	Number of lines	Number of OTM Clients
1	5	10,800	
2	5	10,800	
3	3	6,480	20
4	2	4,400	

Table A-8 Maximum configuration for an Option 11C or Succession CSE 1000 network averaging 400 lines per system

Configuration example	Number of Meridian 1 or Succession CSE 1000 systems	Number of lines*	Number of simultaneous OTM Clients
1	26	10,800	
2	26	10,800	
3	26	10,800	20
4	6	2,600	

* Assumes two simultaneous systems.

Configuration calculations

Example 1

Option 81 = 5 Meridian 1 systems or 10,800 lines:

- Routine operation:
 - If administration is done primarily through the OTM Windows interface:
Adds/Moves/Changes = approximately 23.8% CPU utilization
 - If administration is done primarily through the OTM Web interface:
Adds/Moves/Changes = approximately 36% CPU utilization
- Off-hours operation:
 - Station update = 1 record/3 seconds
 - 9 hours = 32,400 seconds
 - $32,400 \text{ seconds} \times 1 \text{ record}/3 \text{ seconds} = 10,800 \text{ records (lines)}$
 - $10,800 \text{ lines}/2000 \text{ lines per system} = \text{approximately 5 Meridian 1 systems}$
- Network bandwidth:
 - Station (peak) operations = 80 kb/second
 - Network = 100 MB/second
 - $\% \text{ usage per system} = 80 \text{ kb/second} / 100 \text{ MB/second} = \text{approximately } 0.1\%$
 - $35\% \text{ allowed usage} / 0.1\% \text{ per system} = \text{approximately 350 Meridian 1 systems}$

Option 11C = 26 Meridian 1 or Succession CSE 1000 systems or 10,800 lines:

- Routine operation:
 - If administration is done primarily through the OTM Windows interface:
Adds/Moves/Changes = approximately 23.8% CPU utilization
 - If administration is done primarily through the OTM Web interface:
Adds/Moves/Changes = approximately 36% CPU utilization
- Off-hours operation:
 - Station update = 1 record/6 seconds
 - 9 hours = 32,400 seconds
 - $32,400 \text{ seconds} * 1 \text{ record}/6 \text{ seconds} = 5,400 \text{ records (lines)}$
 - $5,400 \text{ lines}/400 \text{ lines per system} * 2 \text{ simultaneous systems} =$
approximately 26 Meridian 1 or Succession CSE 1000 systems
- Network bandwidth:
 - Station (peak) operations = 40 kb/second
 - Network = 100 MB/second
 - % usage per system = $40 \text{ kb/second} / 100 \text{ MB/second} =$
approximately 0.05%
 - $35\% \text{ allowed usage} / 0.05\% \text{ per system} =$ approximately 700 Meridian 1
or Succession CSE 1000 systems



Note: The average alarms and MDECT usage are so small that their impact on routine, off-hour, and network bandwidth is negligible.

Example 2

Option 81 = 3 Meridian 1 systems or 6,480 lines:

- Routine operation:
 - If administration is done primarily through the OTM Windows interface:
If Web Desktop Services Write for End Users is not configured, then
Adds/Moves/Changes = approximately 14.28% CPU utilization
If Web Desktop Services Write for End Users is configured, then
Adds/Moves/Changes = approximately 17.88% CPU utilization

- If administration is done primarily through the OTM Web interface:
If Web Desktop Services Write for End Users is not configured, then
Adds/Moves/Changes = approximately 21.6% CPU utilization
If Web Desktop Services Write for End Users is configured, then
Adds/Moves/Changes = approximately 25.2% CPU utilization
- OTM Client usage on OTM Server = approximately 4% per Client
80% CPU time / 4% per Client = 20 OTM Clients
- Off-hours operation:
 - Station update = 1 record/3 seconds
 - OTM Client station update = 1 record/5 seconds
 - LDAP Sync operation = 10 records/second
For 100,000 records = approximately 2.8 hours
 - 9 hours = 32,400 seconds
 - $32,400 \text{ seconds} * 1 \text{ record/3 seconds} = 6,480 \text{ records (lines)}$
 - $6,480 \text{ lines} / 2000 \text{ lines per system} = \text{approximately 3 Meridian 1 systems}$
- Network bandwidth:
 - Station (peak) operations = 80 kb/second
 - LDAP Sync operation = 720 kb/second
Percent usage of network = approximately 0.7%
 - Network = 100 MB/second
 - Percent usage per system = $80 \text{ kb/second} / 100 \text{ MB/second} = \text{approximately 0.1\%}$
 - $35\% \text{ allowed usage} / 0.1\% \text{ per system} = \text{approximately 350 Meridian 1 systems}$

Option 11C = 26 Meridian 1 or Succession CSE 1000 systems or 10,800 lines:

- Routine operation:
 - If administration is done primarily through the OTM Windows interface:
If Web Desktop Services Write for End Users is not configured, then
Adds/Moves/Changes = approximately 23.8% CPU utilization
If Web Desktop Services Write for End Users is configured, then
Adds/Moves/Changes = approximately 29.8% CPU utilization
 - If administration is done primarily through the OTM Web interface:

If Web Desktop Services Write for End Users is not configured, then
Adds/Moves/Changes = approximately 36.0% CPU utilization

If Web Desktop Services Write for End Users is configured, then
Adds/Moves/Changes = approximately 42.0% CPU utilization

- OTM Client usage on OTM Server = approximately 4% per Client
80% CPU time / 4% per Client = 20 OTM Clients
- Off-hours operation:
 - Station update = 1 record/6 seconds
 - OTM Client station update = 1 record/5 seconds
 - LDAP Sync operation = 10 records/second
For 100,000 records = approximately 2.8 hours
 - 9 hours = 32,400 seconds
 - 32,400 seconds * 1 record/6 seconds = 5,400 records (lines)
 - 5,400 lines/400 lines per system * 2 simultaneous systems =
approximately 26 Meridian 1 or Succession CSE 1000 systems
- Network bandwidth:
 - Station (peak) operations = 40 kb/second
 - LDAP Sync operation = 720 kb/second
Percent usage of network = approximately 0.7%
 - Network = 100 MB/second
 - Percent usage per system = 40 kb/second / 100 MB/second =
approximately 0.05%
 - 35% allowed usage / 0.05% per system = approximately 700 Meridian 1
or Succession CSE 1000 systems

Example 3

Option 81 = 2 Meridian 1 systems or 4,400 lines:

- Routine Operation:
 - CDR plus traffic = approximately 3.5% per system
 - If administration is done primarily through the OTM Windows interface:
Adds/Moves/Changes = approximately 9.7% CPU utilization
 - If administration is done primarily through the OTM Web interface:
Adds/Moves/Changes = approximately 14.67% CPU utilization

- Off-hours operation:
 - Parsing plus Cost Report = 20 records/second
 - 18 hours of call collection operation = 64,800 seconds
 - $64,800 \text{ seconds} * 3 \text{ call records/second/system} = 194,400 \text{ call records per system}$
 - 6 hours of report generation = 21,600 seconds
 - $21,600 \text{ seconds} * 20 \text{ records/second} = 432,000 \text{ call records in 6 hours}$
 - $432,000 \text{ call records} / 194,400 \text{ call records per system} =$
approximately 2 Meridian 1 systems
- Network bandwidth:
 - CDR plus traffic (peak) operations = 118 kb/second
 - Network = 100 MB/second
 - Percent usage per system = $118 \text{ kb/second} / 100 \text{ MB/second} =$
approximately 0.1%
 - $35\% \text{ allowed usage} / 0.1\% \text{ per system} =$
approximately 350 Meridian 1 systems

Option 11C = 6 Meridian 1 or Succession CSE 1000 systems or 2,600 lines:

- Routine operation:
 - If administration is done primarily through the OTM Windows interface:
Adds/Moves/Changes = approximately 5.73% CPU utilization
 - If administration is done primarily through the OTM Web interface:
Adds/Moves/Changes = approximately 8.67% CPU utilization
- Off-hours operation:
 - Parsing plus Cost Report = 20 records/second
 - 18 hours of call collection operation = 64,800 seconds
 - $64,800 \text{ seconds} * 1 \text{ call record/second/system} = 64,800 \text{ call records per system}$
 - 6 hours of report generation = 21,600 seconds
 - $21,600 \text{ seconds} * 20 \text{ records/second} = 432,000 \text{ call records in 6 hours}$
 - $432,000 \text{ call records at } 64,800 \text{ call records/system} =$
approximately 6 Meridian 1 or Succession CSE 1000 systems

- Network bandwidth:
 - CDR plus traffic (peak) operations = 59 kb/second
 - Network = 100 MB/second
 - Percent usage per system = $59 \text{ kb/second} / 100 \text{ MB/second} =$
approximately 0.05%
 - 35% allowed usage / 0.05% per system = approximately 700 Meridian 1
or Succession CSE 1000 systems

Index

A

- access permissions 160
 - administrators 160
- acronyms 22
- add
 - OTM Web Navigator users 158
 - OTM Windows users 151
 - site 106
- add object to Optivity NMS 214
- adding
 - system
 - Meridian 1 108
 - Succession CSE 1000 127
- Alarm Management, set up 202
- alarms 188, 227
- application executables 59
- applications 51, 55, 63, 69, 104, 217
 - remove 70
- authentication 156

B

- backup 202
- bandwidth A-22

C

- Call Accounting 75, 80
- Call Detail Records. *See* CDR.
- capacity factors A-1
- CDR data 75, 80
- checklist, installation 37

- CLAN. *See* customer LAN.

- common data 51, 60, 67

- communication settings, Terminal Server 199

- configure

- Desktop Services 174

- ITG Line 2.0 data 191, 193

- modem 90

- high-speed smart modem considerations 91

- virtual port 195

- Windows NT

- system settings 255

- workgroups 254

- configure Remote Access Service with TCP/IP 257

- connection, test 98

- conventions, text 22

- custom installation 53, 55

- customer LAN 266, A-19, A-20, A-22

- customer support 26

- customer WAN A-21

- CWAN. *See* customer WAN.

D

- Data Buffering and Access, set up 200

- Database Migration Utility 77

- DBA. *See* Data Buffering and Access.

- default installation 53

- Desktop Services 174, A-9

- dongle 87

E

ELAN. *See* embedded LAN.
embedded LAN A-19, A-20, A-21, A-22
embedded WAN A-20
engineering guidelines A-1
EWAN. *See* embedded WAN.

F

Fault Summary 219
 set up 219
files
 application 51
 common data 51, 60
 local data 52, 61
 OIT 209
 read me 57

G

gatekeeper zones
 managing 146
GCAS. *See* General Cost Allocation System.
General Cost Allocation System A-2

H

hard disk A-15
hardware requirements
 disk size A-16
 HP OpenView 226
 OTM Client 35, 40, A-14
 OTM Server 30, 39, A-12
 OTM stand-alone 39, A-13
 OTM Web Client A-14
 processor speed A-17
HP OpenView 224
 configure OTM Server 247
 hardware and software requirements 226
 installation and configuration 229
 limitations of OTM integration 225

I

i2004 telephone 193
identification 47
InfoCenter 211
installation 71
 custom 53, 55
 default 53
 Desktop Services 174
 HP OpenView 229
 on a MAT file server 76
 options 53
 OTM Client software 58
 OTM Server software 41
 outline 42
 Remote Access Service 256
 Web browser client 204
 Windows 2000 260
 Windows NT 249
 component installation 251, 262
 network adapter software 252
integration
 HP OpenView 224
 Optivity NMS 206
Internet Protocol. *See* IP.
Internet Telephony Gateway. *See* ITG.
IP address, find 188
IP Line card 193
IP telephones 190
ITG Line 2.0 190, 192, 194

J

Java Runtime Environment 57, 204, 210, 218
JRE. *See* Java Runtime Environment.

K

keycode 50, 62, 85

L

- LD 117 186, 188
- LD 17 181
- LDAP Server, set up 201
- license 85
- licenses 67
 - OTM Client 87
 - Reporting Unit 86
 - Terminal Number 85
- Lightweight Directory Access Protocol. *See* LDAP.
- limitations
 - software
 - hard-coded A-3
 - operational A-8
- local data 52, 61
- login 96, 159

M

- M1. *See* Meridian 1.
- MAT. *See* Meridian Administration Tools.
- Media Gateway 193
- Media Gateways 192
- memory requirements A-14
- Meridian 1
 - add system 108
 - programming 38
 - set up 180
 - software requirements 37
- Meridian Administration Tools A-3
 - migration to OTM 75
 - on a different PC 77
 - on a new Windows 2000 PC 78
 - on a PC being upgraded to Windows 2000 78
 - on the same PC 75
 - summary 79
- Meridian Mail A-18
- Microsoft Encrypted Authentication 259
- Migrating CDR data from MAT 80

- modem 264, A-10
 - configuration 90
 - high-speed smart modem considerations 91
 - troubleshooting 92
- Multilink 259

N

- Navigator access 166
- NetWare 36
- network map 226
- Network Node Manager 225
 - access OTM Server 228
 - Alarm Browser 227
 - configure OTM Server 247
 - configure OTM Web Server Access 245
 - event configuration 231
 - network map 226
 - OTM Status Monitor 236
 - set up Network Map 237
- NNM. *See* Network Node Manager.
- Novell 36

O

- OIT files 209
- OIT. *See* Optivity Integration Toolkit.
- oitInstall 210
- Option 11C 190
- Optivity Integration Toolkit 209
- Optivity Network Management System. *See* Optivity NMS.
- Optivity NMS
 - adding OTM Server object 214
 - InfoCenter 211
 - integration requirements 207
 - OIT files 209
 - oitInstall 210
 - start OTM Web applications 217
 - troubleshooting 222
- Optivity NMS, integration 206

Optivity Telephony Manager. *See* OTM.

OTM administrators 159

OTM Client

hardware requirements 35, 40

license 87

software installation 58

software requirements 40

upgrade 66

OTM Directory 175

OTM Help desk users 159

OTM Navigator 106

OTM Server 214

hardware requirements 30, 39

object properties

modifying 217

viewing 216

software installation 41

software requirements 31, 39

upgrade 65, 66

OTM stand-alone

hardware requirements 39

software requirements 39

OTM Status Monitor 236

OTM Web Navigator 158

OTM Windows Navigator 151

overlay. *See* LD.

P

password, change default 96

pcANYWHERE A-18

product support 26

programming, Meridian 1 38

publications

hard copy 26

related 23

R

RAS. *See* Remote Access Service.

read me file 57

Remote Access Service 256, 257

client 259

Remote Access Service (RAS) 264

Reporting Unit license. *See* RU license.

requirements 29

Ethernet connections 37, 180

hardware

Meridian 1 180

OTM Client 40

OTM Server 39

OTM stand-alone 39

OTM Client

hardware 35

OTM Server

hardware 30

software 31

OTM stand-alone

hardware 39

software 39

PPP connections 37, 181

serial connections 38, 181

software

Meridian 1 37

OTM Client 40

OTM Server 39

OTM stand-alone 39

X11 packages 29

X11 system software 29

RU license 86

S

SDI ports 181

security 159

security device 87

serial connection A-18

serial number 50, 85

Server installation requirements 39

set up

Alarm Management 202

- applications 104
- communications information 98
- customer information 103
- Data Buffering and Access 200
- LDAP Server 201
- Meridian 1 180
- Succession CSE 1000 180
- system data 106
- virtual terminal service 195
- Windows 2000 261
- Windows NT 250
- setup choices 48
- site, adding 106
- software installation procedure 43
- Software License Agreement 45
- software requirements
 - HP OpenView 226
 - Meridian 1 29, 37
 - OTM Client 40
 - OTM Server 31, 39
 - OTM stand-alone 39
- stand-alone 39
- Succession Communication Server for Enterprise 1000. *See* Succession CSE 1000.
- Succession CSE 1000 192
 - add system 127
 - set up 180
- support, Nortel Networks 26
- supported systems 28
- supported upgrade paths 28
- survivability 190
- survivable
 - expansion cabinet 190
 - Media Gateway 192
- system
 - add
 - Meridian 1 108
 - Succession CSE 1000 127
- system restart 58

T

- TBS. *See* Telecom Billing System.
- TCP/IP 257, 263
- technical publications 26
- technical support 26
- Telecom Billing System 80
- Telephone access 168
 - Details tab 174
 - Features tab 172
 - General tab 170
 - Keys tab 170
- Telephony Managers folder 215
- Terminal Number license. *See* TN license.
- test
 - connection 98
 - network cards 266
- text conventions 22
- TN license 85
- transmit data to ITG Line 2.0 cards 194
- troubleshooting
 - modem connections 92
 - Optivity NMS 222

U

- uninstall OTM 267
- upgrades 64
 - applications 69
 - existing version of OTM 65
 - OTM PCs to Windows 2000 65
 - OTM Server to same release 65
 - to a new release 66
- user
 - adding 154
 - authentication 156
- user group
 - creating 152
 - properties 167
- users

- Default 159
- OTM administrators 159
- OTM Help desk 159

V

- virtual ports 195

W

- Web browser 204
- Web client 36
- Web Help 71
- Web reporting role 175
- Web Services 71
- Web Station A-8
- welcome screen 46
- Windows 2000 31, 32
 - installing 260
 - setup program 261
- Windows 2000 Professional 32
- Windows 2000 Server 32
- Windows 98 32
- Windows Client performance 35
- Windows NT 31, 32, 65
 - component installation 251, 262
 - configure system settings 255
 - configure workgroups 254
 - Emergency Repair disk 255
 - installing 249
 - network adapter software installation 252
 - setup program 250

X

- X11 packages 29, 37
- X11 system software 29